

Dominion KX II

用户指南
2.3 版

DKX2-v2.3.0-0M-CHS

2010 年 7 月

255-62-4023-00

FCC 信息

本设备经测试符合 FCC 规则第 15 部分规定的 A 类数字设备限制要求。这些限制旨在合理保护商用安装设备免受有害干扰的影响。本设备产生、使用并辐射射频能量，如果不按说明书安装和使用，可能会对无线通信造成有害干扰。在居民区使用本设备可能会造成有害干扰。

VCCI 信息（日本）

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

事故、灾害、误用、滥用、擅自修改产品或其他不受 Raritan 合理控制的事件造成的产品损坏，或者在非正常工作条件下造成的产品损坏，Raritan 均不承担责任。



目录





用户管理 106

设备管理 129



安全管理 189

维护 204

Diagnostics（诊断） 218

命令行界面 225



Dominion KX II Local Console 235

规格 251

更新 LDAP 模式 277

参考资料 285





常见问题解答 298

索引 331



Ch 1 简介

在本章内

Dominion KX II 帮助

Dominion KX II 帮助说明如何安装、设置和配置 Dominion KX II。它还说明如何访问目标服务器和电源条，如何使用虚拟媒体，如何管理用户和安全，如何维护和诊断 Dominion KX II。

可以在 Raritan 网站上的 ***Raritan Firmware and Documentation page（固件和文档页）*** ***http://www.raritan.com/support/firmware-and-documentation/***下载 PDF 版本的帮助。Raritan 建议你浏览 Raritan 网站，了解最新的用户指南。

必须在浏览器上启用 Active Content（活动内容），才能使用联机帮助。如果使用 Internet Explorer 7，必须启用 Scriplets（代码块）。阅读浏览器帮助文件，了解如何启用这些功能。

相关文档

可以在 Raritan 网站上的 ***Raritan Firmware and Documentation page（固件和文档页）*** ***http://www.raritan.com/support/firmware-and-documentation/***找到 Dominion KX II 帮助、Dominion KX II 快速安装指南和 Dominion KX II VMWare 快速安装指南。可以在 **KVM 和串行访问客户机指南**和 Raritan 网站上找到与 Dominion KX II 一起使用的客户机应用程序的安装要求和说明。本帮助在适当的地方说明与 Dominion KX II 一起使用的特定客户机功能。



帮助新增内容

在增强和修改设备和/或用户文档之后，增加了下列信息。

- 现在可以使用级联配置如果使用级联配置，用基础 Dominion KX II 设备访问多台其他级联设备。参看***配置和启用级联*** (p. 137)详细了解级联。
- 现在可以配置供 Dominion KX II 使用的 HTTP 和/或 HTTPS 端口。参看 ***HTTP 和 HTTPS 端口设置*** (p. 136)。
- 增加了安全提示功能，你可以用它创建和显示安全提示，并有选择地要求用户在 Dominion KX II 登录过程中接受或拒绝安全协议。参看***安全提示*** (p. 202)。
- Dominion KX II 支持 P2CIM-APS2DUAL 和 P2CIM-AUSBDUAL CIM，提供两个 RJ45 端口连接不同的 KVM 切换器。参看***支持的 Paragon CIM 和配置*** (p. 261)。
- 在 Port Access（端口访问）页上增加了一个新选项卡，允许你按名称搜索服务器。参看***端口访问页*** (p. 41)。
- 在 AKC 使用帮助中增加了其他必要信息。参看***使用 AKC 的前提*** (p. 80)。
- 现在可以在本地控制台上选择活动的 USB 配置文件。参看***本地控制台 USB 配置文件选项*** (p. 238)。

请参看发布说明，详细了解本版本的帮助发生了哪些变化。



Dominion KX II 概述

Dominion KX II 是企业级安全数字 KVM（键盘、视频和鼠标）切换器，支持在世界上的任何地方通过网络浏览器进行 BIOS 级（及以上）服务器访问和控制。一台标准 Dominion KX II 最多可以控制 64 台服务器。如果使用 Dominion KX II 八用户型，可以用 KX2-832 控制最多 32 台服务器，用 KX2-864 控制最多 64 台服务器。

Dominion KX II 最多支持八个视频通道，最多允许八个并发用户在同一时间连接八台视频目标。在机架上，Dominion KX II 通过一套键盘、监视器和鼠标，最多可以对 64 台服务器和其他 IT 设备进行 BIOS 级控制。Dominion KX II 集成的远程访问功能便于你通过网络浏览器对服务器进行相同级别的控制。

Dominion KX II 很容易用标准 UTP（5/5e/6 类）电缆连接。它的高级功能包括虚拟媒体、128 位加密、双电源、远程电源控制、双 Ethernet、LDAP、RADIUS、Active Directory®、系统日志集成、外置调制解调器功能和 Web 管理。Dominion KX II 八用户设备背面还有一个扩展本地端口。这些功能便于你随时随地延长正常运行时间，提高生产力，加强网络安全。

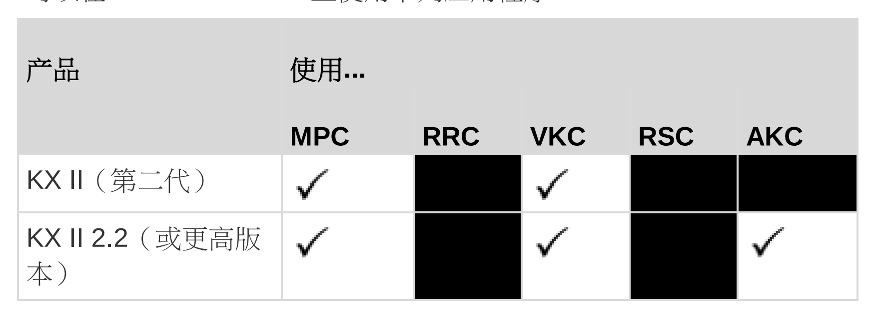
Dominion KX II 产品可以作为独立设备工作，不依赖中央管理设备。对于大型数据中心和大企业，可以使用 Raritan CommandCenter Secure Gateway (CC-SG) 管理工具，将多台 Dominion KX II 设备（与用于串行控制台访问的 Dominion SX 设备和用于远程/分公司管理的 Dominion KSX 设备）集成为一个逻辑解决方案。


Raritan.

图示符号			
1	五类电缆	7	远程虚拟媒体 USB 驱动器
2	计算机接口模块 (CIM)	8	电源条
3	Dominion KX II	9	本地访问 *注意：KX2-832 和 KX2-864 还使用扩展本地端口。*
4	远程 KVM 和串行设备	A	IP LAN/WAN
5	调制解调器	B	PSTN
6	远程（网络）访问		

可与 Dominion KX II 一起使用的客户机应用程序

可以在 Dominion KX II 上使用下列应用程序：



产品	使用...				
	MPC	RRC	VKC	RSC	AKC
KX II（第二代）	✓		✓		
KX II 2.2（或更高版本）	✓		✓		✓

参看 **KVM 和串行客户机指南**了解客户机应用程序详情。同时参看本指南的***如何使用目标服务器*** (p. 36)部分了解如何与 Dominion KX II 一起使用客户机。

注意：MPC 和 VKC 需要 Java™ Runtime Environment (JRE™)。AKC 建立在 .NET 之上。



虚拟媒体

所有 Dominion KX II 设备都支持虚拟媒体。现在所有 Dominion KX II 设备均支持虚拟媒体，即安装在目标服务器上、支持软件安装和诊断的远程驱动器/介质。

每种 Dominion KX II 均配备虚拟媒体，可通过绝大部分 CD、DVD、USB、内置驱动器、远程驱动器和镜像文件完成远程管理任务。与其他解决方案不同的是，Dominion KX II 支持硬盘和远程安装镜像文件的虚拟媒体访问，从而提高灵活性和工作效率。

虚拟媒体会话用 128 位 AES 或 RC4 加密算法加以保护。

D2CIM-VUSB CIM（Computer Interface Module，计算机接口模块）和 D2CIM-DVUSB 支持对那些支持 USB 2.0 接口的 KVM 目标服务器进行虚拟媒体会话。这些 CIM 还支持绝对鼠标同步™和远程固件更新。

注意：DVUSB CIM 上的黑色连接器用于连接键盘和鼠标。灰色连接器用于连接虚拟媒体。让 CIM 的两个插头保持连接设备。如果两个插头不连接目标服务器，设备可能无法正常工作。



产品图片





Dominion KX II



KX2-832



KX2-864





产品特点

硬件

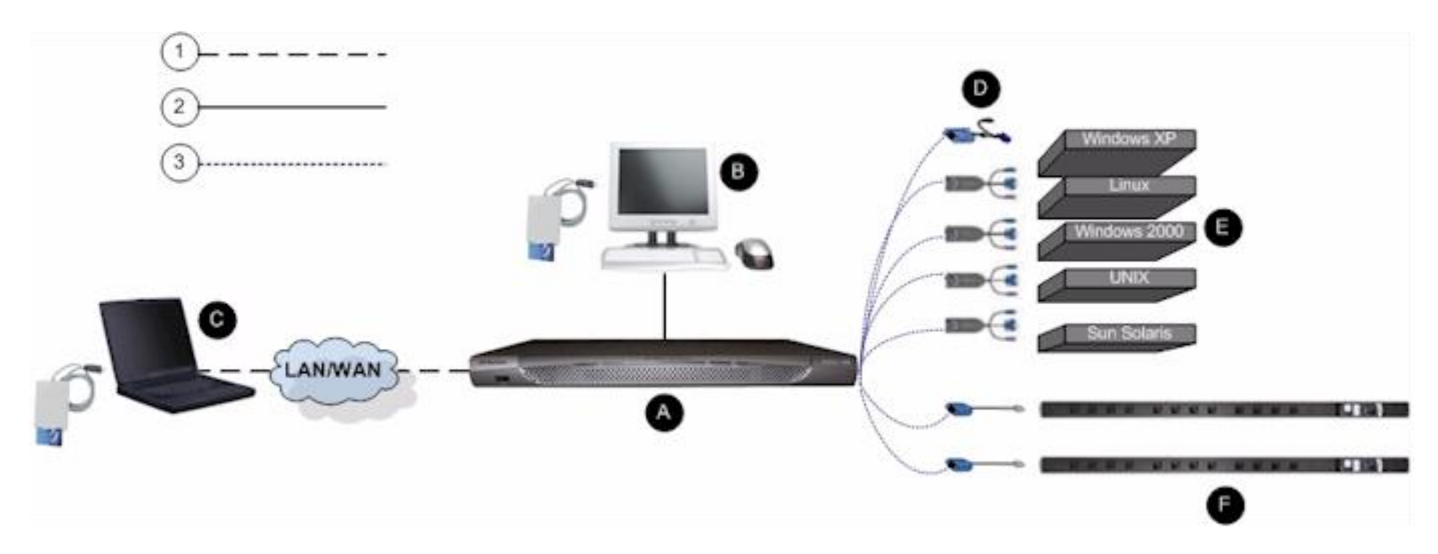
- 集成 KVM-over-IP 远程访问
- 1U 或 2U 机架安装（包括安装托架）
- 具备故障切换功能的双电源；自动切换电源，发出电源故障警报
- 8 个、16 个、32 个或 64 个 (KX2-464) 服务器端口
- 32 个 (KX2-832) 或 64 个 (KX2-864) 服务器端口
- 级联支持如果使用级联配置，用基础 Dominion KX II 设备访问多台其他级联设备。参看***配置和启用级联*** (p. 137)详细了解级联。
- 最多八个视频通道（视设备型号而定），每次最多允许八个用户连接 Dominion KX II
- 多用户能力（1/2/4/8 个远程用户；1 个本地用户）
- UTP（5/5e/6 类）服务器电缆
- 双 Ethernet 端口 (10/100/1000 LAN)，具备故障切换功能
- 现场升级
- 在机架上访问所用的本地用户端口
  - PS/2 键盘/鼠标端口。KX2-832 和 KX2-864 只有 USB 端口。
  - 前面板和背板上分别有一个和三个支持 USB 设备的 USB 2.0 端口
  - 全面支持远程用户并发访问
  - 本地管理图形用户界面
- 扩展本地端口在机架上扩展 KX2 设备访问
- 集中访问安全
- 集成电源控制
- 双电源状态、网络活动和远程用户状态 LED 指示灯
- 硬件复位按钮
- 用于连接外置调制解调器的串行端口

软件

- D2CIM-VUSB 和 D2CIM-DVUSB CIM 虚拟媒体
- D2CIM-VUSB CIM 和 D2CIM-DVUSB CIM 绝对鼠标同步
- 即插即用
- Web 访问和管理
- 直观图形用户界面
- KVM 信号（包括视频和虚拟媒体）128 位加密
- LDAP、Active Directory®、RADIUS 或内部验证和授权
- 支持 DHCP 自动获得或固定 IP 设置
- 智能卡/CAC 验证
- SNMP 和系统日志管理
- IPv4 和 IPv6 支持
- 与服务器直接关联、旨在防止错误的电源控制
- 与 Raritan CommandCenter Secure Gateway (CC-SG) 管理工具集成
- CC Unmanage 功能（使设备不受 CC-SG 控制）

术语

在本手册中，典型 Dominion KX II 配置使用下列组件术语：





图示符号	
1	TCP/IP IPv4 和/或 IPv6
2	KVM（键盘、视频和鼠标）
3	UTP 电缆（5/5e/6 类）
A	Dominion KX II
B	本地访问端口 本地用户 — 与 Dominion KX II 直接相连、直接在机架上（而不是通过网络）用于控制 KVM 目标服务器的可选用户控制台（包括键盘、鼠标和 multisync VGA 监视器）。还可以把本地端口连接的 USB 智能卡读卡器安装在目标服务器上。DKX2-832 和 DKX2-864 设备还有一个扩展本地端口。
C	远程 PC 用于访问和控制与 Dominion KX II 相连的 KVM 目标服务器的联网计算机。还可以通过 Dominion KX II£¬把 USB 智能卡读卡器连接到远程 PC 和目标服务器。
D	CIM 插在每台目标服务器或电源条上的 dongle。可用于所有支持的操作系统。
E	目标服务器 KVM 目标服务器 — 通过 Dominion KX II 远程访问、有显示卡和用户界面（例如 Windows® 操操作系统、Linux®、Solaris™ 等）的服务器。
F	Dominion PX 电源条 通过 Dominion KX II 远程访问的 Raritan 电源条。

参看***支持的 CIM 和操作系统（目标服务器）*** (p. 255)了解 Dominion KX II 支持的操作系统和 CIM 清单，参看***支持的操作系统（客户机）*** (p. 264)了解支持的操作系统清单。

包装内容

每台 Dominion KX II 是全配置的标准 1U 独立产品，可以安装在标准的 1U（DKX2-864 为 2U）19" 机架安装机箱上。每台 Dominion KX II 设备包括下列零部件：

包装数量	品名
1	Dominion KX II 设备
1	Dominion KX II 快速安装指南
1	机架安装套件
1	交流电源线
1	五类网线
1	五类交叉网线
1	4 个橡胶垫（用于桌面安装）
1	应用说明
1	保修卡



Ch 2 安装和配置

在本章内

概述

本节简要概述安装过程，本章后面的各节详细说明每个步骤。

► 安装和配置 **Dominion KX II：**

- ***第一步：配置 KVM 目标服务器*** (p. 14)
- ***第二步：配置网络防火墙设置*** (p. 25)
- ***第三步：连接设备*** (p. 26)
- ***第四步：配置 Dominion KX II*** (p. 29)
- ***第五步（可选）：配置键盘语言*** (p. 34)

本节还要介绍所需的默认登录信息，尤其是默认 IP 地址、用户名和密码。参看***默认登录信息*** (p. 13)。

默认登录信息

默认值	值
用户名	默认用户名是 admin。此用户有管理权。
密码	默认密码是 raritan。 密码区分大小写，必须按在创建密码时使用的大小写输入密码。例如默认密码 raritan 必须全部按小写字母输入。 在首次启动 Dominion KX II 时，必须更改默认密码。
IP address（IP 地址）	Dominion KX II 默认 IP 地址是 192.168.0.192。

重要说明：为备用和业务连续性起见，我们强烈建议你创建一个备用管理员用户名和密码，并将它们保存在安全的地方。



入门

第一步：配置 KVM 目标服务器

KVM 目标服务器是要通过 Dominion KX II 访问和控制的服务器。在安装 Dominion KX II 之前，先配置所有 KVM 目标服务器，确保服务器具备最佳性能。此配置只适用于 KVM 目标服务器，不适用于在远程访问 Dominion KX II 时所用的客户机工作站（远程 PC）。参看***术语*** (p. 10)了解其他信息。

桌面背景

为了使带宽效率和视频性能最佳，运行 Windows®、Linux®、X-Windows、Solaris™ 和 KDE 等图形用户界面的目标服务器需要配置。桌面背景不必是纯色，但如果用照片或复杂渐变图片作为桌面背景，可能会使性能下降。

鼠标设置

Dominion KX II 可以在几种鼠标模式下工作：

- 绝对鼠标模式™（仅限于 D2CIM-VUSB）
- 智能鼠标（不使用动画鼠标）
- 标准鼠标模式

不必针对绝对鼠标同步修改鼠标参数，但此模式需要 D2CIM-VUSB 或 D2CIM-DVUSB。标准鼠标模式和智能鼠标模式的鼠标参数必须设置为特定值，本手册将介绍这些设置。在不同的目标操作系统上，鼠标配置会有差异。参看操作系统文档了解详情。

大多数 Windows 操作系统通常能很好地支持智能鼠标模式。如果在目标服务器上设置活动桌面，智能鼠标模式可能会造成无法预测的后果。如要详细了解智能鼠标模式设置，参看***智能鼠标模式*** (p. 70)。

在刀片服务器机箱上安装了内置 KVM 切换器的服务器，通常不支持绝对鼠标技术。

Windows 7、Windows XP、Windows 2003 和 Windows 2008 设置

► **配置运行 Microsoft® Windows 7® 操作系统、Windows XP® 操作系统、Windows 2003® 操作系统或 Windows 2008® 操作系统的 KVM 目标服务器：**

1. 配置鼠标设置：
   a. 选择 Start（开始）> Control Panel（控制面板）> Mouse（鼠标）。
   b. 单击 Pointer Options（指针选项）选项卡。



c. 在 Motion（移动）组上：

- 将 Mouse Motion Speed（鼠标移动速度）准确设置为中速。
- 禁用 Enhance pointer precision（增强指针精度）选项。
- 禁用 Snap To（捕捉）选项。
- 单击 OK（确定）按钮。

注意：在目标服务器上运行 Windows 2003 时，如果通过 KVM 访问服务器并执行下列任何操作，即使前面启用了鼠标同步，也可能会失去鼠标同步。为了再次启用鼠标同步，必须在客户机的 Mouse（鼠标）菜单上选择 Synchronize Mouse（同步鼠标）命令。下列操作可能会导致失去鼠标同步：

- 打开文本编辑器。

- 在 Windows Control Panel（控制面板）上访问 Mouse Properties（鼠标属性）、Keyboard Properties（键盘属性）和 Phone and Mode（电话和模式）选项。

---

2. 禁用过渡效果：

   a. 在 Control Panel（控制面板）上选择 Display（显示）。

   b. 单击 Appearance（外观）选项卡。

   c. 单击 Effects（效果）按钮。

   d. 取消 Use the following transition effect for menus and tooltips（菜单和工具提示使用下列过渡效果）选项。

   e. 单击 OK（确定）按钮。

3. 关闭 Control Panel（控制面板）。

注意：对于运行 Windows XP、Windows 2000 或 Windows 2008 的 KVM 目标服务器，你可能要创建一个仅用于通过 Dominion KX II 建立远程连接的用户名。这样，可以将目标服务器的低速鼠标指针移动/加速度设置仅限于 Dominion KX II 连接。

Windows XP、2000 和 2008 登录页恢复到预设的鼠标参数，这些参数不同于为实现最佳 Dominion KX II 性能而建议的参数。因此，鼠标同步对这些屏幕而言可能不是最佳方案。

警告！只有在你正确调整 Windows 目标服务器上的注册表之后，才继续下一步。可以用 Windows 注册表编辑器更改下列设置，使 Dominion KX II 在登录页上具有更好的鼠标同步性能：HKey_USERS\.DEFAULT\Control Panel\Mouse: > MouseSpeed = 0;MouseThreshold 1=0;MouseThreshold 2=0。

Windows 2000 设置

▶ 配置运行 Microsoft® Windows 2000® 操作系统的 KVM 目标服务器：

1. 配置鼠标设置：
   a. 选择 Start（开始）> Control Panel（控制面板）> Mouse（鼠标）。
   b. 单击 Motion（移动）选项卡。
      - 将 Acceleration（加速度）设置为 None（无）。
      - 将 Mouse Motion Speed（鼠标移动速度）准确设置为中速。
      - 单击 OK（确定）按钮。
2. 禁用过渡效果：
   a. 在 Control Panel（控制面板）上选择 Display（显示）。
   b. 单击 Effects（效果）选项卡。
      - 取消 Use the following transition effect for menus and tooltips（菜单和工具提示使用下列过渡效果）选项。
3. 单击 OK（确定）按钮，关闭 Control Panel（控制面板）。

注意：对于运行 Windows XP、Windows 2000 或 Windows 2008 的 KVM 目标服务器，你可能要创建一个仅用于通过 Dominion KX II 建立远程连接的用户名。这样，可以将目标服务器的低速鼠标指针移动/加速度设置仅限于 Dominion KX II 连接。

Windows XP、2000 和 2008 登录页恢复到预设的鼠标参数，这些参数不同于为实现最佳 Dominion KX II 性能而建议的参数。因此，鼠标同步对这些屏幕而言可能不是最佳方案。

警告！只有在你正确调整 Windows 目标服务器上的注册表之后，才继续下一步。可以用 Windows 注册表编辑器更改下列设置，使 Dominion KX II 在登录页上具有更好的鼠标同步性能：HKey_USERS\.DEFAULT\Control Panel\Mouse: > MouseSpeed = 0;MouseThreshold 1=0;MouseThreshold 2=0。

Windows Vista 设置

▶ 配置运行 Windows Vista® 操作系统的 KVM 目标服务器：

1. 配置鼠标设置：
   a. 选择 Start（开始）> Settings（设置）> Control Panel（控制面板）> Mouse（鼠标）。
   b. 单击 Pointer Options（指针选项）选项卡。
   c. 在 Motion（移动）组上：



- 将 Mouse Motion Speed（鼠标移动速度）准确设置为中速。
- 禁用 Enhanced pointer precision（增强指针精度）选项。
- 单击 OK（确定）按钮。

2. 禁用动画和淡化效果：
   a. 在 Control Panel（控制面板）上选择 System（系统）选项。
   b. 选择 Performance Information（性能信息），然后选择 Tools（工具）> Advanced Tools（高级工具）> Adjust（调节），调节 Windows 外观和性能。
   c. 单击 Advanced（高级）选项卡。
   d. 单击 Performance（性能）组里的 Settings（设置）按钮，打开 Performance Options（性能选项）对话框。
   e. 在 Custom（定制）选项下取消下列复选框：
   - 动画选项：
     - Animate controls and elements inside windows（窗口用动画显示控件和元素）
     - Animate windows when minimizing and maximizing（在最大化和最小化窗口时用动画显示窗口）
   - 淡化选项：
     - Fade or slide menus into view（在视图中淡化或滑动菜单）
     - Fade or slide ToolTips into view（在视图中淡化或滑动工具提示）
     - Fade out menu items after clicking（在单击后让菜单项淡出）
3. 单击 OK（确定）按钮，关闭 Control Panel（控制面板）。

Linux 设置 (Red Hat 9)

注意：下列设置仅对标准鼠标模式进行过优化。

▶ 配置运行 Linux® 的 KVM 目标服务器（图形用户界面）：

1. 配置鼠标设置：
   a. 选择 Main Menu（主菜单）> Preferences（首选项）> Mouse（鼠标）。打开 Mouse Preferences（鼠标首选项）对话框。
   b. 单击 Motion（移动）选项卡。
   c. 在 Speed（速度）组上将 Acceleration（加速度）滑动条准确置于正中央。
   d. 在 Speed（速度）组上降低 Sensitivity（灵敏度）。



e. 在 Drag & Drop（拖放）组上降低 Threshold（阈值）。

f. 关闭 Mouse Preferences（鼠标首选项）对话框。

注意：如果这些步骤不起作用，按照 Linux 命令行说明书中的说明，在命令行上发出 xset mouse 1 1 命令。

---

2. 配置屏幕分辨率：

   a. 选择 Main Menu（主菜单）> System Settings（系统设置）> Display（显示）。打开 Display Settings（显示设置）对话框。

   b. 在 Display（显示）选项卡上选择 Dominion KX II 支持的分辨率。

   c. 在 Advanced（高级）选项卡上验证 Dominion KX II 支持的刷新率。

注意：一旦连接目标服务器，在许多 Linux 图形环境下用 <Ctrl> <Alt> <+> 命令更改视频分辨率，滚动显示在 XF86Config 或 /etc/X11/xorg.conf 文件里启用的所有可用分辨率，视你的 X 服务器分发版本而定。

▶ 配置运行 Linux 的 KVM 目标服务器（命令行）：

1. 将 Mouse Acceleration（鼠标加速度）准确设置为 1，将 Threshold（阈值）准确设置为 1。输入此命令：*xset mouse 1 1*。这些设置在登陆后执行。
2. 确保运行 Linux 的每台目标服务器使用 Dominion KX II 支持的分辨率（采用标准 VESA 分辨率和刷新率）。
3. 还应该设置每台 Linux 目标服务器，使消隐时间在 VESA 标准值的 +/-40% 之内：

   a. 转到 Xfree86 配置文件 XF86Config。

   b. 用文本编辑器禁用 Dominion KX II 不支持的所有分辨率。

   c. 禁用（Dominion KX II 不支持的）虚拟桌面功能。

   d. 检查消隐时间（VESA 标准值的+/-40%）。

   e. 重新启动计算机。



注意：如果更改视频分辨率，必须退出目标服务器再登录，视频设置才生效。

Red Hat 9 KVM 目标服务器注意事项

如果在使用 USB CIM 的目标服务器上运行 Red Hat® 9，键盘和/或鼠标出问题，可以尝试其他配置设置。

提示：即使重新安装操作系统，也可能必须执行这些步骤。

配置使用 USB CIM 的 Red Hat 9 服务器：

1. 在系统里找到配置文件（通常是 /etc/modules.conf）。
2. 使用你喜欢的编辑器，确保 modules.conf 文件里的 alias usb-controller 行如下所示：

   alias usb-controller usb-uhci

   注意：如果 /etc/modules.conf 文件的另一行使用 usb-uhci，必须删除或注释该行。

3. 保存文件。
4. 重新启动系统，更改才会生效。

Linux 设置 (Red Hat 4)

注意：下列设置仅对标准鼠标模式进行过优化。

配置运行 Linux® 的 KVM 目标服务器（图形用户界面）：

1. 配置鼠标设置：
   a. 选择 **Main Menu（主菜单）> Preferences（首选项）> Mouse（鼠标）。打开 Mouse Preferences（鼠标首选项）对话框。**
   b. 打开 Motion（移动）选项卡。
   c. 在 Speed（速度）组上将 Acceleration（加速度）滑动条准确置于正中央。
   d. 在 Speed（速度）组上降低 Sensitivity（灵敏度）。
   e. 在 Drag & Drop（拖放）组上降低 Threshold（阈值）。
   f. 关闭 Mouse Preferences（鼠标首选项）对话框。

   注意：如果这些步骤不起作用，按照 Linux 命令行说明书中的说明，在命令行上发出 xset mouse 1 1 命令。

2. 配置屏幕分辨率：

a. 选择 Main Menu(主菜单)> System Settings(系统设置)> Display（显示）。打开 Display Settings（显示设置）对话框。

b. 在 Setting（设置）选项卡上选择 Dominion KX II 支持的分辨率。

c. 单击 OK（确定）按钮。

注意：一旦连接目标服务器，在许多 Linux 图形环境下用 <Ctrl> <Alt> <+> 命令更改视频分辨率，滚动显示在 XF86Config 或 /etc/X11/xorg.conf 文件里启用的所有可用分辨率，视你的 X 服务器分发版本而定。

注意：如果更改视频分辨率，必须退出目标服务器再登录，视频设置才生效。

SUSE Linux 10.1 设置

注意：切勿尝试在 SUSE Linux® 登录提示下同步鼠标。必须连接目标服务器，才能同步鼠标光标。

配置鼠标设置：

1. 选择 **Desktop（桌面）> Control Center（控制中心）。打开 Desktop Preferences（桌面首选项）对话框。**
2. 单击 Mouse（鼠标）。打开 Mouse Preferences（鼠标首选项）对话框。
3. 打开 Motion（移动）选项卡。
4. 在 Speed（速度）组上将 Acceleration（加速度）滑动条准确置于正中央。
5. 在 Speed（速度）组上降低 Sensitivity（灵敏度）。
6. 在 Drag & Drop（拖放）组上降低 Threshold（阈值）。
7. 单击 Close（关闭）按钮。

配置视频：

1. 选择 Desktop Preferences（桌面首选项）> Graphics Card and Monitor（显示卡和监视器）。打开 Card and Monitor Properties（显示卡和监视器属性）对话框。
2. 确定 Dominion KX II 是否支持目前使用的分辨率和刷新率。参看***支持的视频分辨率*** (p. 268)了解详情。

   注意：如果更改视频分辨率，必须退出目标服务器再登录，视频设置才生效。



永久保存 Linux 设置

注意：对于不同版本的 Linux®，这些步骤可能会有少许差异。

▶ 永久保存 Linux 设置（提示）：

1. 选择 System Menu（系统菜单）> Preferences（首选项）> Personal（个人）> Sessions（会话）。
2. 单击 Session Options（会话选项）选项卡。
3. 选择 Prompt on log off（在退出时提示）复选框，单击 OK（确定）按钮。当你退出时，此选项提示你保存当前会话。
4. 在退出之后，在对话框上选择 Save current setup（保存当前设置）选项。
5. 单击 OK（确定）按钮。

提示：如果不希望在退出时提示，执行下列步骤。

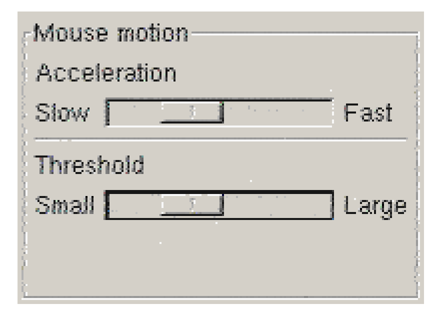
▶ 永久保存 Linux 设置（不提示）：

1. 选择 Desktop（桌面）> Control Center（控制中心）> System（系统）> Sessions（会话）。
2. 单击 Session Options（会话选项）选项卡。
3. 取消 Prompt on log off（在退出时提示）复选框。
4. 选择 Automatically save changes to the session（自动保存会话更改）复选框，单击 OK（确定）按钮。当你退出时，此选项自动保存当前会话。

Sun Solaris 设置

▶ 配置运行 Sun™ Solaris™ 的 KVM 目标服务器：

1. 将 Mouse Acceleration（鼠标加速度）值精确设置为 1，将 Threshold（阈值）精确设置为 1。可以这样设置：
   - 图形用户界面。



   - 在命令行输入 *xset mouse a t*，其中 a 是加速度，t 是阈值。



2. 必须将所有目标服务器配置为 Dominion KX II 支持的其中一个显示分辨率。Sun 机器支持的常用分辨率如下：

显示分辨率	垂直刷新率	纵横比
1600 x 1200	60 Hz	4:3
1280 x 1024	60,75,85Hz	5:4
1152 x 864	75 Hz	4:3
1024 x 768	60,70,75,85Hz	4:3
800 x 600	56,60,72,75,85Hz	4:3
720 x 400	85 Hz	9:5
640 x 480	60,72,75,85Hz	4:3

3. 运行 Solaris 操作系统的目标服务器必须输出 VGA 视频（水平和垂直同步，而不是复合同步）。

▶ 将 Sun 显示卡输出从复合同步更改成非默认的 VGA 输出：

1. 发出 Stop+A 命令进入 bootprom 模式。
2. 发出下列命令更改输出分辨率：*setenv output-device screen:r1024x768x70*
3. 发出 `boot` 命令重新启动服务器。

也可以联系 Raritan 代表购买视频输出适配器：

如果你有：	使用此视频输出适配器：
采用复合同步输出的 Sun 13W3	APSSUN II Guardian 转换器
采用复合同步输出的 Sun HD15	1396C 转换器（把 HD15 转换成 13W3）和 APSSUN II Guardian 转换器（支持复合同步）
采用分离同步输出的 Sun HD15	APKMSUN Guardian 转换器

注意：在某些 Sun 服务器上，某些标准的 Sun 背景屏幕可能不精确居中，有黑边现象。使用另一个背景，或者在左上角放一个浅色图标。

鼠标设置

▶ 配置鼠标设置 (Sun Solaris 10.1)：

1. 选择 Launcher（启动器）。打开 Application Manager（应用程序管理器）— Desktop Controls（桌面控制）。



2. 选择 Mouse Style Manager（鼠标式样管理器）。打开 Style Manager - Mouse（式样管理器 — 鼠标）对话框。
3. 将 Acceleration（加速度）滑动条设置为 1.0。
4. 将 Threshold（阈值）滑动条设置为 1.0。
5. 单击 OK（确定）按钮。

访问命令行

1. 单击右键。
2. 单击 Tools（工具）> Terminal（终端）。打开终端窗口。（最好在根目录下发出命令。）

视频设置 (POST)

Sun 系统有两种不同的分辨率设置：POST 分辨率和 GUI 分辨率。在命令行上运行这些命令。

注意：这里用 1024x768x75 举例说明，取代你使用的分辨率和刷新率。

▶ 检查当前 POST 分辨率：

- 在根目录下运行下列命令：`# eeprom output-device`

▶ 更改 POST 分辨率：

1. 运行 `# eeprom output-device=screen:r1024x768x75`。
2. 退出或重新启动计算机。

视频设置 (GUI)

GUI 分辨率可用不同的命令检查和设置，取决于所用的显示卡。在命令行上运行这些命令。

注意：这里用 1024x768x75 举例说明，取代你使用的分辨率和刷新率。

显示卡	检查分辨率：	更改分辨率：
32 位	# /usr/sbin/pgxconfig -prconf	1. # /usr/sbin/pgxconfig -res 1024x768x75 2. 退出或重新启动计算机。
64 位	# /usr/sbin/m64config -prconf	1. # /usr/sbin/m64config -res 1024x768x75 2. 退出或重新启动计算机。
32 位和 64 位	# /usr/sbin/fbconfig -prconf	1. # /usr/sbin/fbconfig -res 1024x768x75 2. 退出或重新启动计算机。

IBM AIX 5.3 设置

根据下列步骤配置运行 IBM® AIX™ 5.3 的 KVM 目标服务器。

▶ 配置鼠标：

1. 转到 Launcher（启动器）。
2. 选择 Style Manager（式样管理器）。
3. 单击 Mouse（鼠标）。打开 Style Manager - Mouse（式样管理器 — 鼠标）对话框。
4. 用滑动条将 Mouse acceleration（鼠标加速度）设置为 1.0，将 Threshold（阈值）设置为 1.0。
5. 单击 OK（确定）按钮。

▶ 配置视频：

1. 在启动器上选择 Application Manager（应用程序管理器）。
2. 选择 System_Admin（系统管理）。
3. 选择 Smit > Devices（设备）> Graphic Displays（图形显示）> Select the Display Resolution and Refresh Rate（选择显示分辨率和刷新率）。
4. 选择使用的显示卡。
5. 单击 List（列表）。显示显示模式列表。
6. 选择 Dominion KX II 支持的分辨率和刷新率。参看***支持的视频分辨率*** (p. 268)了解详情。

注意：如果更改视频分辨率，必须退出目标服务器再登录，视频设置才生效。



*永久保存 **UNIX** 设置*

注意：对于使用的不同的 UNIX®（例如 Solaris™ 和 IBM® AIX™）和特定版本，这些步骤可能会有少许差异。

---

1. 选择 **Style Manager（式样管理器）> Startup（启动）。打开 Style Manager - Startup（式样管理器 — 启动）对话框。**
2. 在 Logout Confirmation（退出确认）对话框上选择 On（开）选项。当你退出时，此选项提示你保存当前会话。

***Apple Macintosh* 设置**

对于运行 Apple Macintosh® 操作系统的 KVM 目标服务器，首选方法是使用 D2CIM-VUSB 和绝对鼠标同步。

注意：必须在 USB Profile（USB 配置文件）菜单或 Port Configuration（端口配置）页上选择 USB Profile Mac OS-X v10.4.9 和更高版本。

第二步：配置网络防火墙设置

为了用 Multi-Platform Client 通过网络防火墙或 Port Access（端口访问）页访问 Dominion KX II，防火墙必须允许通过 TCP 端口 5000 或你指定的另一个端口进行通信。

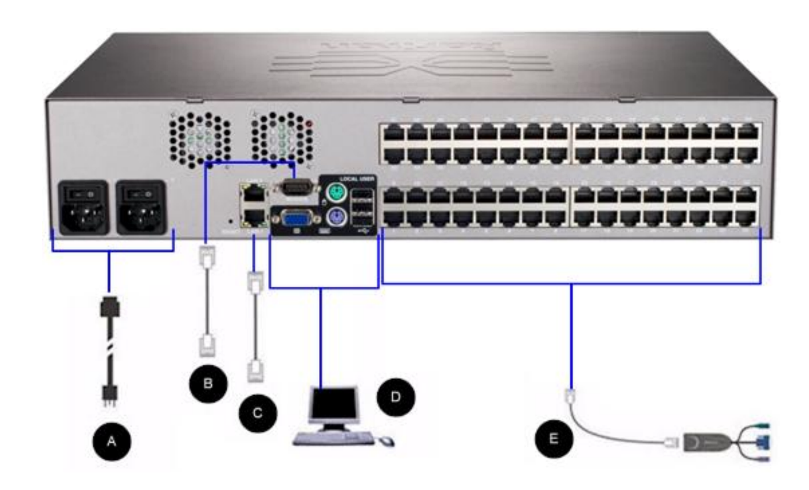
利用 **Dominion KX II**：	**防火墙必须允许通过下列端口进行入站通信：**
Web 访问能力	端口 443 — 用于 HTTPS 通信的标准 TCP 端口
HTTP 请求自动重定向到 HTTPS（所以可以使用更常用的 http://xxx.xxx.xxx.xxx，而不是 https://xxx.xxx.xxx.xxx）	端口 80 — 用于 HTTP 通信的标准 TCP 端口

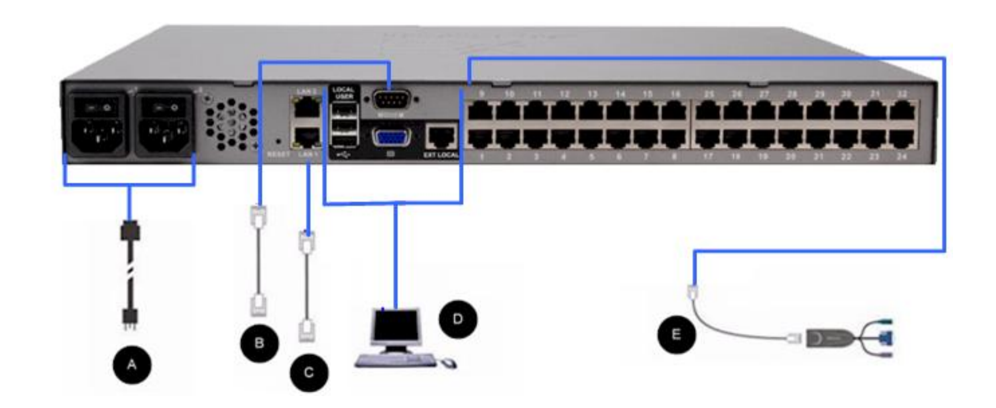
参看***网络设置*** (p. 129)，进一步了解如何指定另一个发现端口。



第三步：连接设备

将 Dominion KX II 连接到电源、网络、本地 PC 和目标服务器。图中的字母对应介绍此连接的章节。





A. 交流电源

▶ 连接电源：

1. 将随附的交流电源线接到 Dominion KX II 上，将另一端插入交流电源插座。
2. 为了实现双电源故障切换保护，将随附的第二根交流电源线接到 Dominion KX II 上，将另一端插入与第一根电源线不同的电源插座。

注意：如果只连接一根电源线，Dominion KX II 面板上的电源 LED 指示灯显示红色，这是因为系统设置为自动检测两个电源。 *参看***电源设置** *(p. 152)，了解如何关闭未使用电源的自动检测。*



B. 调制解调器端口（可选）

Dominion KX II 有一个专用调制解调器接口，在 LAN/WAN 不可用时用于进行远程访问。用直通串行 (RS-232) 电缆将外置调制解调器连接到 Dominion KX II 背板上的 MODEM 端口（参看***规格*** (p. 251)了解经过认证的调制解调器清单，参看***配置调制解调器设置*** (p. 143)了解如何配置调制解调器）。

注意：Raritan 建议你通过启用 CD（载波检测）设置来配置调制解调器。

C. 网络端口

Dominion KX II 有两个 Ethernet 端口，用于故障切换（而非负载平衡）。在默认情况下，只有 LAN1 处于活动状态，禁用自动故障切换。在启用自动故障切换之后，如果 Dominion KX II 内部网络接口或相连的网络切换器不可用，将启用 LAN2，使用相同的 IP 地址。

注意：由于只有在实际发生故障之后才激活故障切换端口，所以 Raritan 建议你不要监视故障切换端口，或者只有在发生故障切换之后才监视该端口。

▶ 连接网络：

1. 用随附的标准 Ethernet 电缆连接标记为 LAN1 的网络端口与 Ethernet 交换器、集线器或路由器。
2. 使用可选的 Dominion KX II Ethernet 故障切换功能：
   - 用一根标准 Ethernet 电缆连接标记为 LAN2 的网络端口与 Ethernet 交换器、集线器或路由器。
   - 在 Network Configuration（网络配置）页上启用 Automatic Failover（自动故障切换）。

注意：只有在将其中一个网络端口用作故障切换端口时，才使用两个网络端口。

D. 本地访问端口（本地 PC）

为便于访问机架上的目标服务器，使用 Dominion KX II Local Access（本地访问）端口。虽然安装和设置需要本地访问端口，但它在后续使用中是任选的。本地访问端口还通过 Dominion KX II Local Console 提供图形用户界面，便于进行管理访问和目标服务器访问。

KX2-832 和 KX2-864 设备背面还有一个标有 EXT LOCAL 字样的 Extended Local（扩展本地）端口，用于访问机架上的目标服务器。在首次安装和设置时，不需要 Extended Local(扩展本地)端口。可以在 Local Console 和 Remote Console 上配置它。 参看***配置 Dominion KX II 本地端口设置*** (p. 185)了解详情。

- 连接本地端口：

- 使用 PS/2 或 USB 键盘和鼠标，把 multisync VGA 监视器、鼠标和键盘连接到各自的 Local User（本地用户）端口（DKX2-832 和 DKX2-864 只有 USB 端口）。Local User（本地用户）端口和 Extended Local（扩展本地）端口物理连接位于 Dominion KX II 背板上。

连接	说明
监视器	将标准 multisync VGA 监视器连接到 HD15（母）视频端口。
键盘	将标准 PS/2 键盘连接到 Mini-DIN6（母）键盘端口，或者将标准 USB 键盘连接到 USB Type A（母）端口。
鼠标	将标准 PS/2 鼠标连接到 Mini-DIN6（母）鼠标端口，或者将标准 USB 鼠标连接到 USB Type A（母）端口。

E. 目标服务器端口

Dominion KX II 用标准 UTP 电缆（5/5e/6 类）连接每台目标服务器。

- 将目标服务器连接到 Dominion KX II：

1. 使用合适的计算机接口模块 (Computer Interface Module, CIM)。 参看***支持的 CIM 和操作系统（目标服务器）*** (p. 255)，了解与每个操作系统一起使用的 CIM。



2. 将 CIM 的 HD15 视频连接器插入目标服务器的视频端口。确保目标服务器的视频已配置为支持的分辨率和刷新率。对于 Sun 服务器，还要确保目标服务器的显示卡已设置为输出标准 VGA（水平和垂直同步），而不是复合同步。
3. 将 CIM 的键盘/鼠标连接器插入目标服务器的相应端口。用标准直通 UTP（5/5e/6 类）电缆将 CIM 连接到 Dominion KX II 设备背面的可用服务器端口。

注意：DCIM-USB G2 在 CIM 的背面有一个很小的滑动开关。对于 PC 型 USB 目标服务器，把滑动开工打到 P 位置。对于 Sun USB 目标服务器，把滑动开工打到 S 位置。

只有在给 CIM 重新通电之后，新切换器位置才会生效。如要给 CIM 重新通电，取下目标服务器上的 USB 连接器，稍后再插回去几秒钟。

第四步：配置 Dominion KX II

在首次接通 Dominion KX II 设备电源时，必须通过 Dominion KX II Local Console 进行某些初始配置：

- 更改默认密码。
- 分配 IP 地址。
- 命名 KVM 目标服务器。

更改默认密码

Dominion KX II 配有默认密码。在首次启动 Dominion KX II 时，需要更改默认密码。

▶ 更改默认密码：

1. 按设备背面的电源开关接通 Dominion KX II 电源。等待 Dominion KX II 设备启动。（嘟嘟声表示启动完成）。
2. 在设备启动之后，与 Dominion KX II 本地端口相连的监视器显示 Dominion KX II Local Console。输入默认用户名 (admin) 和密码 (raritan)，然后单击 Login（登录）。显示 Change Password（更改密码）屏幕。
3. 在 Old Password（旧密码）字段里输入旧密码 (raritan)。
4. 在 New Password（新密码）字段里输入新密码，在 Confirm New Password（确认新密码）字段里再次输入新密码。密码最长为 64 个字符，可以包含英文字母数字字符和特殊字符。
5. 单击 Apply（应用）按钮。
6. 显示确认信息，说明密码更改成功。单击 OK（确定）按钮。打开 Port Access（端口访问）页。

注意：也可以在 Raritan Multi-Platform Client (MPC) 上更改默认密码。

分配 IP 地址

下列步骤说明如何在 Network Settings（网络设置）页上分配 IP 地址。如要全面了解本页上的所有字段和操作，参看***网络设置*** (p. 129)。

1. 选择 Device Settings（设备设置）> Network（网络）。打开 Network Settings（网络设置）页。
2. 给 Dominion KX II 设备指定有意义的设备名称。最长 32 个字母数字字符，可以使用有效特殊字符，但不能使用空格。
3. 在 IPv4 部分输入或选择合适的 IPv4 网络设置：
   a. 必要时输入 IP Address（IP 地址）。默认 IP 地址是 192.168.0.192。
   b. 输入 Subnet Mask（子网掩码）。默认子网掩码是 255.255.255.0。
   c. 如果在 IP Auto Configuration（IP 自动配置）下拉列表上选择了 None（无），输入 Default Gateway（默认网关）。
   d. 如果在 IP Auto Configuration（IP 自动配置）下拉列表上选择了 DHCP，输入 Preferred DHCP Host Name（首选 DHCP 主机名）。
   e. 选择 IP Auto Configuration（IP 自动配置）。有三个选项可供选择：
   - None (Static IP)（无[静态 IP]）— 此选项要求你人工指定网络参数。

     建议你选择此选项，因为 Dominion KX II 是基础设施设备，其 IP 地址不应发生变化。
   - DHCP — 联网计算机（客户机）用 Dynamic Host Configuration Protocol（动态主机配置协议）获取 DHCP 服务器分配的唯一 IP 地址和其他参数。

     如果选择此选项，网络参数由 DHCP 服务器指定。如果使用 DHCP，输入 Preferred host name（首选主机名）（仅限于 DHCP）。最长 63 个字符。
4. 如果要使用 IPv6，在 IPv6 部分输入或选择合适的 IPv6 网络设置：
   a. 选择 IPv6 复选框，激活这部分的字段。
   b. 输入 Global/Unique IP Address（全局/唯一 IP 地址）。这是给 Dominion KX II 分配的 IP 地址。
   c. 输入 Prefix Length（前缀长度）。这是 IPv6 地址使用的位数。
   d. 输入 Gateway IP Address（网关 IP 地址）。



e. Link-Local IP Address（链路-本地 IP 地址）。自动给设备分配此地址。用于发现邻居，或者在没有路由器时使用。**只读**

f. 域 ID。标识与此地址关联的设备。**只读**

g. 选择 IP Auto Configuration（IP 自动配置）。有三个选项可供选择：

- None（无）— 如果不想使用自动 IP 配置，而是自己设置 IP 地址（静态 IP），就使用此选项。这是默认选项，建议使用此选项。

  如果给 IP auto configuration（IP 自动配置）选择 None（无），启用下列网络基本设置字段：Global/Unique IP Address（全局/唯一 IP 地址）、Prefix Length（前缀长度）和 Gateway IP Address（网关 IP 地址），你可以人工设置 IP 配置。

- Router Discovery（路由器发现）— 用于选项自动分配 IPv6 地址，这些地址具有 Global（全局）或 Unique Local（唯一本地）意义，超出了 Link Local（链路本地）的意义，仅应用于直接连接的子网。

5. 如果选择了 DHCP，启用了 Obtain DNS Server Address（获取 DNS 服务器地址），就选择 Obtain DNS Server Address Automatically（自动获取 DNS 服务器地址）。在选择 Obtain DNS Server Address Automatically（自动获取 DNS 服务器地址）之后，将使用 DHCP 服务器提供的 DNS 信息。

6. 如果选择了 Use the Following DNS Server Addresses（使用下列 DNS 服务器地址），无论是否选择了 DHCP，均用在此输入的地址连接 DNS 服务器。

   如果选择了 Use the Following DNS Server Addresses（使用下列 DNS 服务器地址）选项，输入下列信息。这些地址分别是主 DNS 地址和备用 DNS 地址，当主 DNS 服务器连接由于中断而断开时，将使用备用 DNS 地址。

   a. Primary DNS Server IP Address（主 DNS 服务器 IP 地址）

   b. Secondary DNS Server IP Address（备用 DNS 服务器 IP 地址）

7. 在填写完之后，单击 OK（确定）按钮。现在 Dominion KX II 设备可通过网络访问了。

参看 ***LAN 接口设置*** (p. 132)，了解如何配置 Network Settings（网络设置）页的这个部分。

---

*注意：在某些环境下，默认 LAN Interface Speed & Duplex setting Autodetect (autonegotiator)（LAN 接口速度和全双工设置自动检测[自动协商]）并不能正确设置网络参数，从而引发网络问题。在这些情况下，将 Dominion KX II LAN Interface Speed & Duplex（LAN 接口速度和全双工）设置为 100 Mbps/Full Duplex（全双工）或与网络相适应的其他选项，可以解决这个问题。参看***网络设置** *(p. 129)页了解详情。*



命名目标服务器

▶ 命名目标服务器：

1. 连接所有目标服务器（如果尚未连接）。参看*第三步：连接设备* (p. 26)，了解如何连接设备。
2. 在 Dominion KX II Local Console 上选择 Device Settings（设备设置）> Port Configuration（端口配置）。打开 Port Configuration（端口配置）页。
3. 单击要重新命名的目标服务器的 Port Name（端口名称）。打开 Port（端口）页。
4. 给与该端口相连的服务器指定一个名称。名称最长为 32 个字符，可以使用字母数字字符和特殊字符。
5. 单击 OK（确定）按钮。

为目标服务器设置相应的名称

字符	说明	字符	说明
!	感叹号	;	分号
"	双引号	=	等号
#	英镑符号	>	大于号
$	美元符号	?	问号
%	百分号	@	@ 符号
&	& 符号	[	左方括号
(	左圆括号	\	反斜杠
)	右圆括号	]	右方括号
*	星号	^	^ 符号
+	加号	_	下划线
,	逗号	`	重音符号
-	短划线	{	左花括号
.	句号	|	管道符
/	斜杠	}	右花括号
<	小于号	~	代字号
:	冒号		



指定电源自动检测

Dominion KX II 有两个电源，可以自动检测这些电源的状态并发出通知。正确配置电源，确保在一个电源发生故障时，Dominion KX II 能发送相应的通知。

配置 Power Supply Setup（电源设置）页，在使用双电源时自动检测两个电源。如果在配置中只使用一个电源，可以在 Power Supply Setup（电源设置）页上禁用自动检测。

▶ 针对使用的电源启用自动检测：

1. 选择 Device Settings（设备设置）> Power Supply Setup（电源设置）。打开 Power Supply Setup（电源设置）页。
2. 如果把电源输入线插入一号电源（设备背面最左边的电源），选择 PowerIn1 Auto Detect（电源输入 1 自动检测）选项。
3. 如果把电源输入线插入二号电源（设备背面最右边的电源），选择 PowerIn2 Auto Detect（电源输入 2 自动检测）选项。
4. 单击 OK（确定）按钮。

注意：如果选择任一个复选框，但实际上并没有连接电源输入，设备面板上的电源 LED 指示灯变成红色。

▶ 对不使用的电源禁用电源自动检测：

1. 在 Dominion KX II Local Console 上选择 Device Settings（设备设置）> Power Supply Setup（电源设置）。打开 Power Supply Setup（电源设置）页。
2. 取消不使用的电源对应的自动检测复选框。

参看***电源设置*** (p. 152)了解详情。

CC-SG 用户注意事项

如果在 CC-SG 配置中使用 Dominion KX II，执行安装步骤，在安装结束之后阅读 **CommandCenter Secure Gateway 用户指南**、**CommandCenter Secure Gateway 管理员指南**或 **CommandCenter Secure Gateway 部署指南**（均可在 Raritan 网站 www.raritan.com 的 Support（支持）页上找到），然后继续下一步。

注意：本帮助中的其余章节主要适用于部署 Dominion KX II 设备，但不集成 CC-SG 功能。



远程验证

CC-SG 用户注意事项

在用 CommandCenter Secure Gateway 控制 Dominion KX II 的情况下，CC-SG 验证用户和组，只有需要本地端口访问的本地用户除外。当 CC-SG 控制 Dominion KX II 时，根据在 Dominion KX II 上配置的本地用户数据库或远程验证服务器（LDAP/LDAPS 或 RADIUS）验证本地端口用户。不根据 CC-SG 用户数据库验证这些用户。

如要进一步了解 CC-SG 验证，参看 CommandCenter Secure Gateway 用户指南、CommandCenter Secure Gateway 管理员指南或 CommandCenter Secure Gateway 部署指南，这些指南均可在 ***Raritan*** *网站* ***http://www.raritan.com***的 Support（支持）页上找到。

支持的协议

为了简化用户名和密码管理，Dominion KX II 可以将验证请求转发到外部验证服务器。支持两种外部验证协议：LDAP/LDAPS 和 RADIUS。

Microsoft Active Directory 注意事项

Microsoft® Active Directory® 在本机使用 LDAP/LDAPS 协议，可以充当 LDAP/LDAPS 服务器和 Dominion KX II 验证源。如果 Microsoft Active Directory 有 IAS (Internet Authorization Server) 组件，Microsoft Active Directory 服务器还可以充当 RADIUS 验证源。

创建用户组和用户

为了让用户访问 Dominion KX II，必须定义用户组和用户，这是初始配置的一部分。

Dominion KX II 使用系统提供的默认用户组，允许你根据需要创建组，并指定适当的权限。

用户名和密码必须能访问 Dominion KX II。当用户尝试访问 Dominion KX II 时，要用这些信息验证用户。

参看用户管理，详细了解如何添加和编辑用户组和用户。

第五步（可选）：配置键盘语言

注意：如果使用美国/国际英语键盘，不需要执行此步骤。

如果使用美国英语之外的语言，必须将键盘配置为适当的语言。此外，客户机和 KVM 目标服务器的键盘语言必须相同。

参看操作系统文档，进一步了解如何更改键盘布局。



更改键盘布局代码（Sun 目标服务器）

如果使用 DCIM-SUSB，要将键盘布局更改为另一种语言，执行此步骤。

▶ 更改键盘布局代码（仅限于 DCIM-SUSB）：

1. 在 Sun™ 工作站上打开 Text Editor（文本编辑器）窗口。
2. 检查 Num Lock 键是否处于激活状态，按键盘上的左 Ctrl 键和 Del 键。Caps Lock 指示灯开始闪烁，表示 CIM 处于 Layout Code Change（布局代码更改）模式。文本窗口显示：`Raritan Computer, Inc. Current keyboard layout code = 22h (US5 UNIX)`（`Raritan Computer, Inc`。当前键盘布局代码 `= 22h (US5 UNIX)`）。
3. 输入期望的布局代码（例如 *31* 表示日文键盘）。
4. 按 Enter 键。
5. 关闭设备，再接通设备电源。DCIM-SUSB 执行复位操作（重新通电）。
6. 确认显示的字符是否正确。



Ch 3　如何使用目标服务器

在本章内

界面

Dominion KX II 有几种用户界面，便于你随时随地访问。这些界面包括 Dominion KX II Local Console、Dominion KX II Remote Console 和 Multi-Platform Client (MPC)。下表说明这些界面，以及它们在目标服务器本地/远程访问和管理中的应用：

用户界面	本地		远程	
	Access（访问）	**Admin（管理员）**	**Access（访问）**	**Admin（管理员）**
Dominion KX II Local Console	✓	✓		
Dominion KX II Remote Console			✓	✓
Virtual KVM Client			✓	
Multi-Platform Client (MPC)			✓	✓
Active KVM Client (AKC)			✓	✓

本帮助中的下列各节介绍如何用特定界面访问 Dominion KX II 并管理目标服务器：

- Local Console
- Remote Console
- Virtual KVM Client
- Multi-Platform Client



Dominion KX II Local Console 界面

在服务器机架上进行访问时，Dominion KX II 通过 Dominion KX II Local Console 提供标准 KVM 管理。Dominion KX II Local Console 提供一个直接 KVM（模拟）连接来连接相连的服务器，其性能犹如你直接连接服务器键盘端口、鼠标端口和视频端口。

Dominion KX II Local Console 图形用户界面和 Dominion KX II Remote Console 图形用户界面有许多相似之处。凡是有差异的地方，本帮助都加以说明。

Dominion KX II Local Console 有 Dominion KX II Local Console Factory Reset（出厂复位）选项，但 Dominion KX II Remote Console 没有此选项。

Dominion KX II Remote Console 界面

Dominion KX II Remote Console 是基于浏览器的图形用户界面，便于你登录与 Dominion KX II 相连的 KVM 目标服务器和串行目标，远程管理 Dominion KX II。

Dominion KX II Remote Console 提供一个数字连接来连接相连的 KVM 目标服务器。在用 Dominion KX II Remote Console 登录 KVM 目标服务器时，打开 Virtual KVM Client 窗口。

Dominion KX II Local Console 图形用户界面和 Dominion KX II Remote Console 图形用户界面有许多相似之处，凡是有差异的地方，本用户手册都加以说明。Dominion KX II Remote Console 有下列选项，但 Dominion KX II Local Console 没有这些选项：

- 虚拟媒体
- 收藏夹
- 备份/恢复
- 固件升级
- 升级报告
- 诊断
- USB 配置文件选择
- USB 配置文件管理
- SSL 证书

启动 Dominion KX II Remote Console

重要说明：无论使用哪种浏览器，都必须允许 Dominion 设备的 IP 地址弹出窗口，这样才能启动 Dominion KX II Remote Console。



由于浏览器和安全设置不同，你可能会看到不同的安全和证书警告消息。必须接受这些警告消息，才能启动 Dominion KX II Remote Console。

你可以在安全和证书警告消息对话框上选择下列选项，减少在以后登录过程中显示的警告消息数量：

- 以后不再显示此警告。
- 始终信任来自此发布者的内容。

启动 Dominion KX II Remote Console：

1. 登录到与 Dominion KX II 相连、安装了 Java Runtime Environment 的任何工作站（JRE 可以在 ***Java 网站 http://java.sun.com/*** 下载）。
2. 启动支持的网络浏览器，例如 Internet Explorer (IE) 或 Firefox。
3. 输入下列 URL： *http://IP-ADDRESS*，其中 IP-ADDRESS 是您给 Dominion KX II 分配的 IP 地址。也可以使用 https，管理员分配的 Dominion KX II DNS 名称（假定配置了 DNS 服务器），或者只在浏览器地址栏输入 IP 地址（Dominion KX II 始终将 IP 地址由 HTTP 重定向到 HTTPS）。打开 Login（登录）页。
4. 输入用户名和密码。如果这是首次登录，用出厂前默认用户名 (admin) 和默认密码（raritan，全部小写）登录。系统提示你更改默认密码。参看***更改默认密码*** (p. 29)了解详情。单击 Login（登录）。

注意：如果管理员要求你在访问设备之前阅读并/或接受安全协议，在你输入登录证书并单击 Login（登录）按钮之后显示安全提示。

参看 ***Virtual KVM Client*** (p. 52)，了解在 Remote Console 上可用的 Dominion KX II 功能。

接口和导航

Dominion KX II 控制台布局

Dominion KX II Remote Console 界面和 Dominion KX II Local Console 界面均提供一个 HTML (Web) 界面，用于配置、管理、目标服务器列表和选择等目的。这些选项位于各个选项卡上。

在成功登录之后，打开 Port Access（端口访问）页，列出所有端口及其状态和可用性。本页有两个选项卡，你可以按端口或按组查看端口及其状态和可用性。可以单击列标题，按 Port Number（端口号）、Port Name（端口名称）、Status (Up and Down)（状态[工作或停止]）和 Availability (Idle, Connected, Busy, Unavailable, and Connecting)（可用性[空闲、已连接、忙、不可用和正在连接]排序端口。参看***端口访问页*** (p. 41)了解详情。



左面板

Dominion KX II 界面左面板包含下列信息：注意某些信息是有条件的，只有在你是某类用户并使用某些功能时，才显示这些信息。在此注明这些有条件信息。

信息	说明	何时显示？
Time & Session（时间和会话）	当前会话的开始日期和时间。	始终
User（用户）	用户名	始终
State（状态）	闲置或活动应用程序的当前状态。如果应用程序闲置，它跟踪并显示会话闲置了多少时间。	始终
Your IP（你的 IP）	访问 Dominion KX II 所用的 IP 地址。	始终
Last Login（上次登录）	上次登录日期和时间。	始终
Under CC-SG Management（受 CC-SG 管理）	负责管理 Dominion KX II 的 CC-SG 设备的 IP 地址。	当 Dominion KX II 受 CC-SG 管理时。
Device Information（设备信息）	你使用的 Dominion KX II 的特定信息。	始终
Device Name（设备名称）	给设备指定的名称。	始终
IP Address（IP 地址)	Dominion KX II 的 IP 地址。	始终
Firmware（固件）	当前固件版本。	始终
Device Model（设备型号）	Dominion KX II 的型号。	始终
Network（网络）	给当前网络指定的名称。	始终
PowerIn1	电源 1 接口连接的状态。要么是开，要么是关。	在连接时。
PowerIn2	电源 2 接口连接的状态。要么是开，要么是关。	在连接时。



信息	说明	何时显示？
Configured As Base or Configured As Tiered（配置为基础或配置为级联）	如果使用级联配置，说明你访问的 Dominion KX II 设备是基础设备还是级联设备。	当 Dominion KX II 是级联配置的组成部分时。
Port States（端口状态）	Dominion KX II 正在使用的端口的状态。	始终
Connect Users（连接用户）	用用户名和 IP 地址标识的、当前连接 Dominion KX II 的用户。	始终
Help - User Guide（帮助 — 用户指南）	联机帮助链接。	始终
Favorite Devices（收藏夹设备）	参看***管理收藏夹*** (p. 44)。	始终
FIPS Mode（FIPS 模式）	FIPS 模式：启用 SSL 证书：符合 FIPS 模式。	在启用 FIPS 时。

Dominion KX II 控制台导航

Dominion KX II 控制台界面有多种导航方法和选择方法。

▶ 选择一个选项（使用下列其中一种方法）：

- 单击一个选项卡。显示一页可用选项。
- 让光标停留在选项卡上，在菜单上选择合适的选项。
- 在分层显示的菜单（浏览路径）上直接选择选项。

▶ 多屏幕页面翻页：

- 使用键盘上的 Page Up 和 Page Down 键。
- 使用右边的滚动条。



端口访问页

在成功登录 Dominion KX II Remote Console 之后，打开 Port Access（端口访问）页。本页列出所有 Dominion KX II 端口、相连的 KVM 目标服务器、及其状态和可用性。Port Access（端口访问）页提供与 Dominion KX II 相连的 KVM 目标服务器的访问。KVM 目标服务器是要通过 Dominion KX II 设备访问和控制的服务器。它们连接 Dominion KX II 背板上的端口。

注意：对于每个 KVM 目标服务器连接，打开一个新的 Virtual KVM Client 页。

如果使用级联配置，用基础 Dominion KX II 设备访问多台其他级联设备，单击基础设备名称左边的展开箭头图标 ，在 Port Access（端口访问）页上查看级联设备。 如果使用级联配置，用基础 Dominion KX II 设备访问多台其他级联设备，单击基础设备名称左边的展开箭头图标 ▶，在 Port Access（端口访问）页上查看级联设备。 参看***配置和启用级联*** (p. 137)详细了解级联。

Port Access（端口访问）页还显示在 Dominion KX II 上配置的刀片服务器机箱。Port Access（端口访问）页采用可展开的分层形式显示刀片服务器机箱，刀片服务器机箱位于分层结构的根部，根下面显示各个有标号的刀片服务器。单击根机箱旁边的展开箭头图标显示各个刀片服务器。

注意：如要按分层顺序查看刀片服务器机箱，必须给刀片服务器机箱配置刀片服务器机箱子类型。

Port Access（端口访问）页默认显示 View by Port（按端口查看）选项卡。View by Group（按组查看）选项卡显示端口组，可以展开显示给此端口组指定的端口。 View by Search（按搜索结果查看）选项卡允许你按端口名称进行搜索。搜索功能支持星号 (*) 通配符、全名和部分名称。

▶ 使用端口访问页：

1. 单击 Dominion KX II Remote Console 上的 Port Access（端口访问）选项卡。打开 Port Access（端口访问）页。

   KVM 目标服务器最初按 Port Number（端口号）排序。可以更改显示方式，按任何一列排序。

   - Port Number（端口号）— 从 1 到 Dominion KX II 设备的总端口数进行编号。注意这里不列出与电源条相连的端口，导致 Port Number（端口号）序列不连续。
   - Port Name（端口名称）— Dominion KX II 端口的名称。端口名称最初设置为 Dominion-KX2-Port#，但可以将名称更改为更具说明性的名称。在单击 Port Name（端口名称）链接时，打开 Port Action（端口操作）菜单。

注意：切勿在 Port (CIM) Name（端口 (CIM) 名称）中使用撇号。

- Status（状态）— 目标服务器的标准状态是工作或停止。
- Type（类型）— 服务器或 CIM 的类型。对于刀片服务器机箱，类型可以是 Blade Chassis（刀片服务器机箱）、Blade（刀片服务器）、BladeChassisAdmin 和 BladeChassisURL。类型还包括级联的设备和 KVM 交换机。
- Availability（可用性）— 可用性可以是 Idle（空闲）、Connected（已连接）、Busy（忙）或 Unavailable（不可用）。当刀片服务器连接工作时，刀片服务器的可用性可以是 shared（共享）或 exclusive（独占）。

2. 单击 View by Port（按端口查看）、View by Group（按组查看）或 View by Search（按搜索结果查看），在不同的视图之间来回切换。
3. 单击要访问的目标服务器的 Port Name（端口名称）。打开 Port Action（端口操作）菜单。参看**端口操作菜单** (p. 43)详细了解可用菜单项。
4. 在 Port Action（端口操作）菜单上选择期望的菜单命令。

更改显示排序顺序：

- 单击要按哪一列排序。按该列排序 KVM 目标服务器列表。

Home > Ports

Port Access

Click on the individual port name to see allowable operations.
0 of 2 Remote KVM channels currently in use.

View By Port | View By Group | View By Search

▲ No.	Name	Type	Status	Availability
1	se-kx2-232-local-port	DCIM	up	idle
2	Dominion_KX2_Port2	Not Available	down	idle
3	► se-kx2-108	TierDevice	up	idle
4	Paragon Port	Not Available	down	idle
5	Ubuntu-Server	Not Available	down	idle
6	Dominion_KX2_Port6	Not Available	down	idle
7	Dominion_KX2_Port7	Not Available	down	idle
8	Dominion_KX2_Port8	Not Available	down	idle
9	▼ ACME-16-Port-KVM	KVMSwitch	down	idle
9-1	ACME-16-Port-KVM-Target-1	KVMSwitchPort	-	-
9-2	ACME-16-Port-KVM-Target-2	KVMSwitchPort	-	-
9-3	KVM_Switch_Port9_Target3	KVMSwitchPort	-	-
9-4	KVM_Switch_Port9_Target4	KVMSwitchPort	-	-
9-5	KVM_Switch_Port9_Target5	KVMSwitchPort	-	-



端口操作菜单

在单击 Port Access（端口访问）列表上的 Port Name（端口名称）时，打开 Port Action（端口操作）菜单。**选择要针对该端口执行的菜单项。注意 Port Action（端口操作）菜单只列出当前可用的选项，视端口状态和可用性而定：**

- Connect（连接）— 建立至目标服务器的新连接。对于 Dominion KX II Remote Console，打开新的 ***Virtual KVM Client*** (p. 52) 页。对于 Dominion KX II Local Console，显示器切换到目标服务器，从本地用户界面切换过去。为了在本地端口上执行切换，必须显示 Dominion KX II Local Console 界面。也可以在本地端口上使用热键切换。

注意：如果一个端口的所有连接处于忙状态，不能在 Dominion KX II Remote Console 上对此端口使用此选项。

- Switch From（切换自）— 从现有连接切换到所选端口（KVM 目标服务器）。此菜单项只适用于 KVM 目标服务器。只有在打开 Virtual KVM Client 时，才显示此选项。

注意：在 Dominion KX II Local Console 上不能使用此菜单项。

- Disconnect（断开）— 断开此端口，关闭此目标服务器对应的 Virtual KVM Client 页。只有在端口状态是工作和连接或工作和忙时，才能使用此菜单项。

注意：在 Dominion KX II Local Console 上不能使用此菜单项。在本地控制台上断开切换目标的唯一方法是使用热键。

- Power On（通电）— 通过关联电源接口给目标服务器通电。只有在目标服务器有一个或多个电源关联时，才显示此选项。
- Power Off（断电）— 通过关联电源接口断开目标服务器电源。只有在目标服务器有一个或多个电源关联，目标服务器通电（端口状态为工作），用户有权操作此服务时，才显示此选项。
- Power Cycle（重新通电）— 通过关联电源接口给目标服务器重新通电。只有在目标服务器有一个或多个电源关联，用户有权操作此服务时，才显示此选项。



管理收藏夹

有一个收藏夹功能，便于你组织管理和迅速访问常用设备。Favorite Devices（收藏夹设备）部分位于 Port Access（端口访问）页左下角（侧面工具栏），便于你：

- 创建和管理收藏夹设备列表
- 迅速访问常用设备
- 按 Device Name（设备名称）、IP Address（IP 地址）或 DNS hostname（DNS 主机名）列出收藏夹
- 发现子网上的 Dominion KX II 设备（在登录前后）
- 在相连的 KX 设备上获取被发现的 Dominion KX II 设备（在登录之后）

注意：此功能只能在 Dominion KX II Remote Console 上使用，不能在 Dominion KX II Local Console 或 AKC 上使用。

▶ 访问收藏夹 Dominion KX II 设备：

- 单击设备名称（位于 Favorite Devices[收藏夹设备]）下面。打开该设备对应的新浏览器窗口。

▶ 按名称显示收藏夹：

- 单击 Display by Name（按名称显示）。

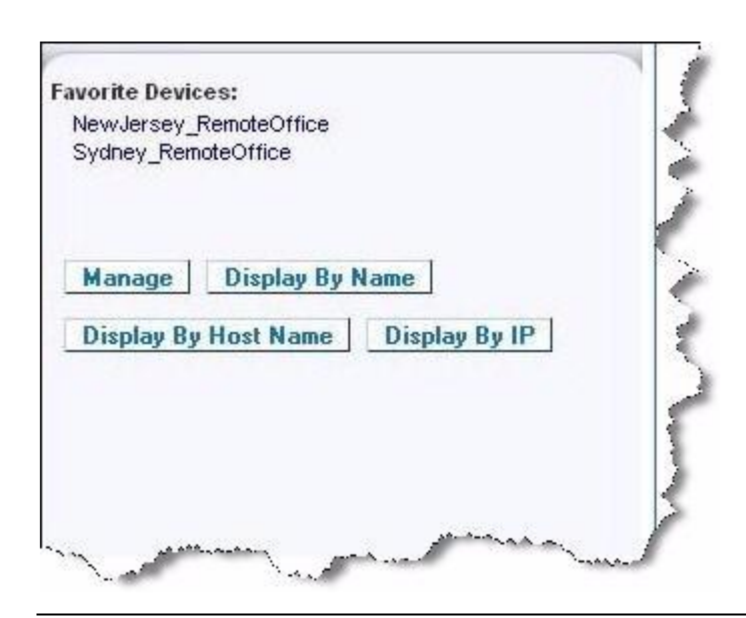
▶ 按 IP 地址显示收藏夹：

- 单击 Display by IP（按 IP 地址显示）。

▶ 按主机名显示收藏夹：

- 单击 Display by Host Name（按主机名显示）。





注意：同时支持 IPv4 地址和 IPv6 地址。

管理收藏夹页

▶ 打开管理收藏夹页：

- 单击左面板上的 Manage（管理）按钮。打开 Manage Favorites（管理收藏夹）页，包含下列选项：

使用：	操作：
Favorites List（收藏夹列表）	管理收藏夹设备的列表。
Discover Devices - Local Subnet（发现设备 — 本地子网）	发现客户机 PC 本地子网上的 Raritan 设备。
Discover Devices - Dominion KX II Subnet（发现设备 — Dominion KX II 子网）	发现 Dominion KX II 设备子网上的 Raritan 设备。
将设备添加到收藏夹	在 Favorites（收藏夹）列表上添加、编辑和删除设备。



收藏夹列表页

在 Favorites List（收藏夹列表）页上，可以在收藏夹列表上添加、编辑和删除设备。

▶ 打开收藏夹列表页：

- 选择 Manage（管理）> Favorites List（收藏夹列表）。打开 Favorites **List（收藏夹列表）页。**

发现本地子网上的设备

此选项发现本地子网上的设备，即 Dominion KX II Remote Console 所在的子网上的设备。可以在本页上直接访问这些设备，也可以将它们添加到收藏夹列表上。参看***收藏夹列表页*** (p. 46)。

▶ 发现本地子网上的设备：

1. 选择 Manage（管理）> Discover Devices（发现设备）— Local Subnet（本地子网）。打开 Discover Devices - Local Subnet（发现设备 — 本地子网）页。
2. 选择合适的发现端口：
   - 如要使用默认发现端口，选择 Use Default Port 5000（使用默认端口 5000）复选框。
   - 如要使用不同的发现端口：

   a. 取消 Use Default Port 5000（使用默认端口 5000）复选框。

   b. 在 Discover on Port（发现端口）字段里输入端口号。

   c. 单击 Save（保存）按钮。
3. 单击 Refresh（刷新）按钮。刷新本地子网设备列表。

▶ 将设备添加到收藏夹列表：

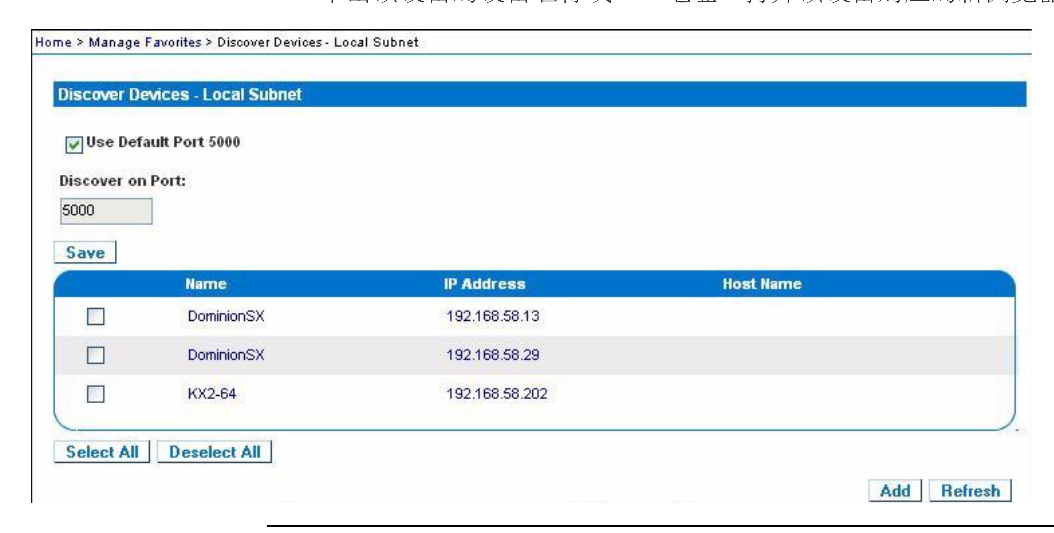
1. 选择设备名称/IP 地址旁边的复选框。
2. 单击 Add（添加）按钮。



提示：用 Select All（全选）按钮和 Deselect All（全部取消）按钮选择或取消远程控制台子网上的所有设备。

▶ 访问被发现的设备：

- 单击该设备的设备名称或 IP 地址。打开该设备对应的新浏览器窗口。

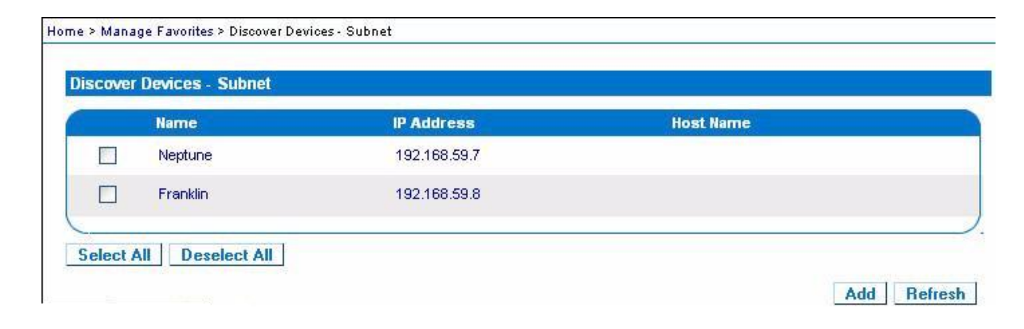


注意：同时支持 IPv4 地址和 IPv6 地址。

发现 Dominion KX II 子网上的设备

此选项发现设备子网上的设备，即 Dominion KX II 设备 IP 地址子网上的设备。可以在本子网页上直接访问这些设备，也可以将它们添加到收藏夹列表上。参看***收藏夹列表页*** (p. 46)。

此功能允许多台 Dominion KX II 设备互操作，自动伸缩。Dominion KX II Remote Console 自动发现 Dominion KX II 子网上的 Dominion KX II 设备和其他任何 Raritan 设备。



发现设备子网上的设备：

1. 选择 **Manage（管理）> Discover Devices（发现设备）— Dominion KX II Subnet（Dominion KX II 子网）。打开 Discover Devices - Dominion KX II Subnet（发现设备 — Dominion KX II 子网）页。**
2. 单击 Refresh（刷新）按钮。刷新本地子网设备列表。

将设备添加到收藏夹列表：

1. 选择设备名称/IP 地址旁边的复选框。
2. 单击 Add（添加）按钮。

提示：用 Select All（全选）按钮和 Deselect All（全部取消）按钮选择或取消 Dominion KX II 设备子网上的所有设备。

访问被发现的设备：

- 单击该设备的设备名称或 IP 地址。打开该设备对应的新浏览器窗口。

注意：同时支持 IPv4 地址和 IPv6 地址。

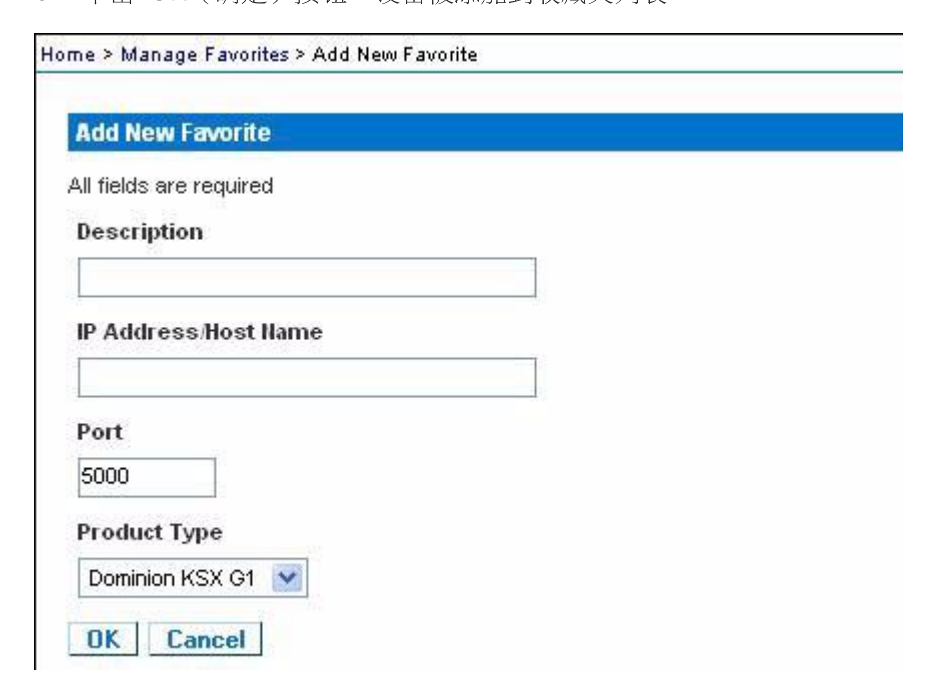
添加、删除和编辑收藏夹

将设备添加到收藏夹列表：

1. 选择 Manage（管理）> Add New Device to Favorites（将新设备添加到收藏夹）。打开 Add New Favorite（添加新收藏夹）窗口。
2. 输入有意义的说明。
3. 输入设备 IP 地址/主机名。
4. 必要时更改发现端口。
5. 选择 Product Type（产品类型）。



6. 单击 OK（确定）按钮。设备被添加到收藏夹列表。



▶ 编辑收藏夹：

1. 在 Favorites List（收藏夹列表）页上选择适当 Dominion KX II 设备旁边的复选框。
2. 单击 Edit（编辑）按钮。打开 Edit（编辑）页。
3. 按需要更新字段：
   - 说明
   - IP Address/Host Name（IP 地址/主机名）— 输入 Dominion KX II 设备的 IP 地址
   - Port（端口，如有必要）
   - Product Type（产品类型）
4. 单击 OK（确定）按钮。

▶ 删除收藏夹：

重要说明：在删除收藏夹时务必要谨慎。系统不提示你确认删除。

1. 选择适当的 Dominion KX II 设备旁边的复选框。
2. 单击 Delete（删除）按钮。收藏夹从收藏夹列表上删除掉。

注意：同时支持 IPv4 地址和 IPv6 地址。

注销

退出 Dominion KX II Remote Console：

- 单击页面右上角的 Logout（退出）。

注意：在退出时，同时关闭打开的任何 Virtual KVM Client 会话和串行客户机会话。

Dominion KX II、MPC、VKC 和 AKC 时的代理服务器配置

在需要使用代理服务器时，必须提供 SOCKS 代理，并在远程客户机 PC 上配置此代理。

注意：如果安装的代理服务器只支持 HTTP 代理协议，不能建立连接。

配置 SOCKS 代理：

1. 在客户机上选择 Control Panel(控制面板)> Internet Options(Internet 选项）。

a. 单击 Connections（连接）选项卡上的 LAN Settings（LAN 设置）。打开 Local Area Network (LAN) Settings（LAN 设置）对话框。

b. 选择 Use a proxy server for your LAN（LAN 使用代理服务器）。

c. 单击 Advanced（高级）。打开 Proxy Settings（代理设置）对话框。

d. 给代理服务器配置所有协议。重要说明：不要选择 Use the same proxy server for all protocols（所有协议使用相同代理服务器）。

注意：SOCKS 代理默认端口 (1080) 不同于 HTTP 代理默认端口 (3128)。

2. 单击每个对话框上的 OK（确定）按钮应用设置。

3. 然后选择 Control Panel（控制面板）> Java，给 Java™ 小程序配置代理。

e. 单击 General（常规）选项卡上的 Network Settings（网络设置）。打开 Network Settings（网络设置）对话框。

f. 选择 Use Proxy Server（使用代理服务器）。

g. 单击 Advanced（高级）。打开 Advanced Network Settings（高级网络设置）对话框。



h. 给代理服务器配置所有协议。重要说明：不要选择 Use the same proxy server for all protocols（所有协议使用相同代理服务器）。

注意：SOCKS 代理默认端口 (1080) 不同于 HTTP 代理默认端口 (3128)。

---

4. 如果使用独立 MPC，还必须：

i. 用文本编辑器打开 MPC 目录下的 start.bat 文件。

j. 在命令行插入下列参数：把它们加在 "-classpath": -DsocksProxyHost=<socks proxy ip addr> -DsocksProxyPort=<socks proxy port> 之前

参数格式如下：

```
start javaw -Xmn128M -Xmx512M -XX:MaxHeapFreeRatio=70
-XX:MinHeapFreeRatio=50 -Dsun.java2d.noddraw=true
-DsocksProxyHost=192.168.99.99 -DsocksProxyPort=1080
-classpath .\sdeploy.jar;.\sFoxtrot.jar;.\jaws.jar;.\sMpc.jar
com.raritan.rrc.ui.RRCApplication %1
```

Multi-Platform Client 界面

Raritan Multi-Platform Client (MPC) 是 Raritan 产品系列的图形用户界面，用于访问那些通过 IP 设备与 Raritan KVM 相连的目标服务器。如要详细了解如何使用 MPC，参看 Raritan 网站上的 **KVM 和串行访问客户机指南**，它与用户指南在同一个网页上。这里说明如何启动 MPC。

在网络浏览器上启动 MPC

重要说明：无论使用哪种浏览器，都必须允许 Dominion 设备的 IP 地址弹出窗口，这样才能打开 MPC。

重要说明：只有使用 Intel® 处理器的 Mac 10.5 和 10.6 能运行 JRE 1.6，可以用做客户机。Mac 10.4.11 和 10.5.8 不支持把 MPC 用做独立客户机。

1. 为了在运行支持的任何浏览器的客户机上打开 MPC，在地址栏输入 http://IP-ADDRESS/mpc，其中 IP-ADDRESS 是 Raritan 设备的 IP 地址。用新窗口打开 MPC。

注意：用 Alt+Tab 命令在本地系统上的窗口之间来回切换。

在打开 MPC 之后，Navigator（导航器）采用树格式显示自动检测的、在子网上找到 Raritan 设备。

2. 如果导航器不按名称列出设备，可以人工添加设备：



a. 选择 Connection（连接）> New Profile（新配置文件）。打开 Add Connection（添加连接）窗口。

b. 在 Add Connection（添加连接）窗口上输入设备 Description（说明），指定 Connection Type（连接类型），添加设备 IP 地址，单击 OK（确定）按钮。可以稍后编辑这些参数。

3. 在页面左边的导航器面板上，用右键单击 Raritan 设备对应的图标连接该设备。

注意：由于浏览器和浏览器安全设置不同，你可能会看到不同的安全和证书复选框和警告消息。为了打开 MPC，必须接受这些选项。

注意：如果使用 FireFox 3.0.3，在启动应用程序时可能会出问题。如有问题，可以清除浏览器高速缓存，再启动应用程序。

Virtual KVM Client

概述

无论何时用 Remote Console 访问目标服务器，都打开 Virtual KVM Client (VKC) 窗口。对于每台连接的目标服务器，均有一个 Virtual KVM Client。可以通过 Windows® 任务栏访问这些窗口。

Virtual KVM Client 窗口可以最小化和最大化，可以在计算机桌面上移动位置。

注意：在刷新 HTML 浏览器时，会关闭 Virtual KVM Client 连接，所以要谨慎。

注意：如果使用 FireFox 3.0.3，在启动应用程序时可能会出问题。如有问题，可以清除浏览器高速缓存，再启动应用程序。

连接 KVM 目标服务器

▶ **连接 KVM 目标服务器：**

1. 单击 Dominion KX II Remote Console 上的 Port Access（端口访问）选项卡。打开 Port Access（端口访问）页。
2. 单击要访问的目标服务器的 Port Name（端口名称）。显示 Port Action（端口操作）菜单。
3. 单击 Connect（连接）。针对与该端口相连的目标服务器打开一个 ***Virtual KVM Client*** (p. 52) 窗口。



VKC 工具栏

注意：KX II-101 VKC 界面不同于其他 Dominion KX 产品的界面。参看 KX II-101 的 VKC 工具栏了解详情。

按钮	按钮名称	说明
	连接属性	打开 Modify Connection Properties（修改连接属性）对话框，可在此人工调节带宽选项（例如连接速度、颜色深度等）。
	视频设置	打开 Video Settings（视频设置）对话框，可在此人工调节视频转换参数。
	颜色校准	调整颜色设置，减少多余的彩色干扰。 与选择 Video（视频）> Color Calibrate（颜色校准）相同。
	目标服务器截屏	单击截取目标服务器图像，将它保存到你选择的文件里。
	同步鼠标	在双鼠标模式下，强制目标服务器鼠标指针与鼠标指针重新对齐。
	刷新屏幕	强制刷新显示屏幕。
	自动检测视频设置	强制刷新视频设置（分辨率和刷新率）。
	智能卡	打开一个对话框，可在与客户机 PC 相连的智能卡读卡器列表上选择智能卡。 *注意：只有 KX II 2.1.10 或更高版本具备此功能。*
	发送 Ctrl+Alt+Del	将 Ctrl+Alt+Del 热键组合发送到目标服务器。
	单光标模式	启动 Single Cursor（单光标）模式，屏幕不再显示本地鼠标指针。 按 Ctrl+Alt+O 退出此模式。 也可以按 Ctrl+左 Alt+M，在快捷菜单上选择 Single/Double Cursor（单/双光标）。
	全屏模式	使屏幕最大化，查看目标服务器桌面。
	缩放比例	增大或缩小目标服务器视频大小，以便在不使用滚动条的情况下看到目标服务器窗口的所有内容。

在 KVM 目标服务器之间切换

可以用 Dominion KX II 访问几种 KVM 目标服务器。Dominion KX II 支持从一台目标服务器切换到另一台目标服务器。

注意：此功能只能在 Dominion KX II Remote Console 上使用。

在 KVM 目标服务器之间切换：

1. 如果已经使用了一台目标服务器，访问 Dominion KX II Port Access（端口访问）页。
2. 单击要访问的目标服务器的端口名称。显示 Port Action（端口操作）菜单。
3. 在 Port Action（端口操作）菜单上选择 Switch From（切换自）选项。Virtual KVM Client 窗口切换到所选的新目标服务器。

控制目标服务器电源

注意：只有在进行电源关联之后，才能使用这些功能。

给 KVM 目标服务器重新通电：

1. 单击 Dominion KX II Remote Console 上的 Port Access（端口访问）选项卡。打开 Port Access（端口访问）页。
2. 单击适当目标服务器的 Port Name（端口名称）。打开 Port Action（端口操作）菜单。
3. 选择 Power Cycle（重新通电）。显示确认消息。

接通目标服务器电源：

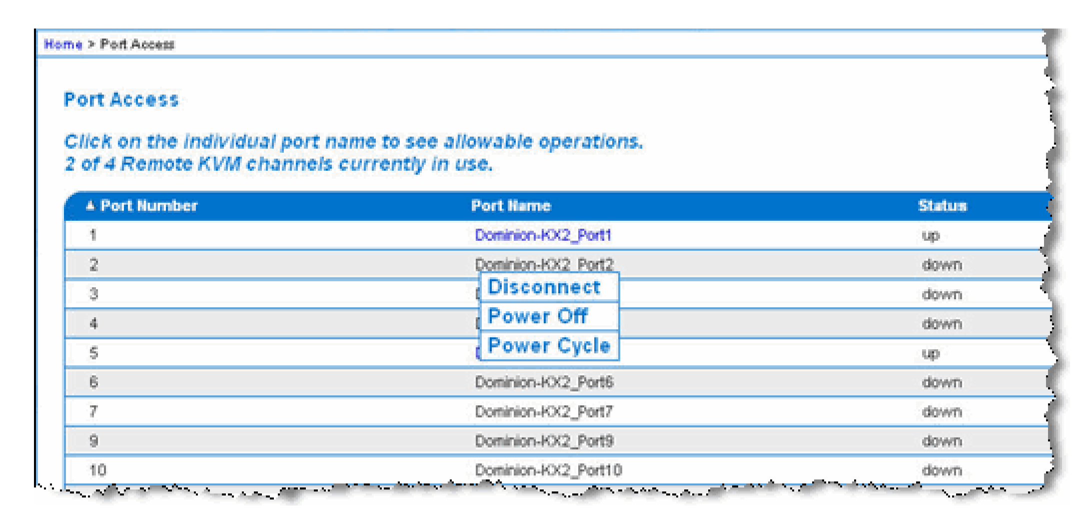
1. 单击 Dominion KX II Remote Console 上的 Port Access（端口访问）选项卡。打开 Port Access（端口访问）页。
2. 单击适当目标服务器的 Port Name（端口名称）。显示 Port Action（端口操作）菜单。
3. 选择 Power On（通电）。显示确认消息。

断开目标服务器电源：

1. 单击 Dominion KX II Remote Console 上的 Port Access（端口访问）选项卡。打开 Port Access（端口访问）页。



2. 单击适当目标服务器的 Port Name（端口名称）。显示 Port Action（端口操作）菜单。
3. 选择 Power Off（断电）。显示确认消息。



断开目标服务器电源

注意：在 Dominion KX II Local Console 上不能使用此菜单项。在本地控制台上断开切换目标的唯一方法是使用热键。

断开目标服务器：

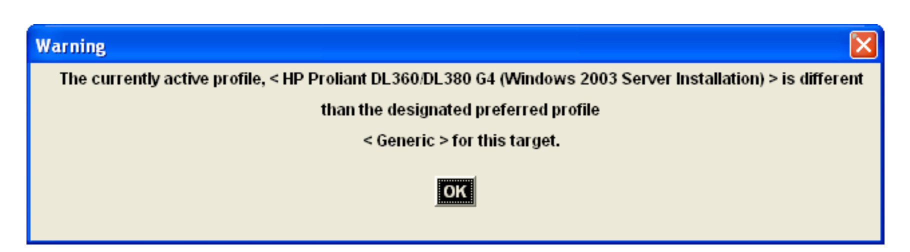
1. 单击要断开的目标服务器的端口名称。显示 Port Action（端口操作）菜单。
2. 选择 Disconnect（断开）。

提示：也可以在 Virtual KVM（虚拟 KVM）菜单上选择 Connection（连接）> Exit（退出），关闭 Virtual KVM Client 窗口。



选择 USB 配置文件

在如***连接 KVM 目标服务器*** (p. 52)所述首次连接 KVM 目标服务器时，自动将首选 USB 配置文件用于端口。如果此前已经用不同的 USB 配置文件连接目标服务器，将使用在上次连接时使用的配置文件。显示类似下面这样的警告消息，告诉你所用的配置文件不是首选配置文件：



在连接目标服务器之后，可以按需要更改 USB 配置文件。VKC 上 USB Profile（USB 配置文件）菜单显示的配置文件很可能就是要使用的配置文件。这些配置文件是管理员预先根据工作需求选择的，用于相连的目标服务器。但是，可以通过 USB Profile（USB 配置文件）菜单上的 Other Profiles（其他配置文件）选项，选择所有配置文件。

▶ 选择 USB 配置文件：

1. 如***连接 KVM 目标服务器*** (p. 52)所述连接 KVM 目标服务器。
2. 在 VKC 上，在 USB Profile（USB 配置文件）菜单上选择一个 USB 配置文件。

   配置文件名称表示该配置文件适用的操作系统或服务器。参看 ***USB 配置文件*** (p. 98)详细了解 USB 配置文件。



连接属性

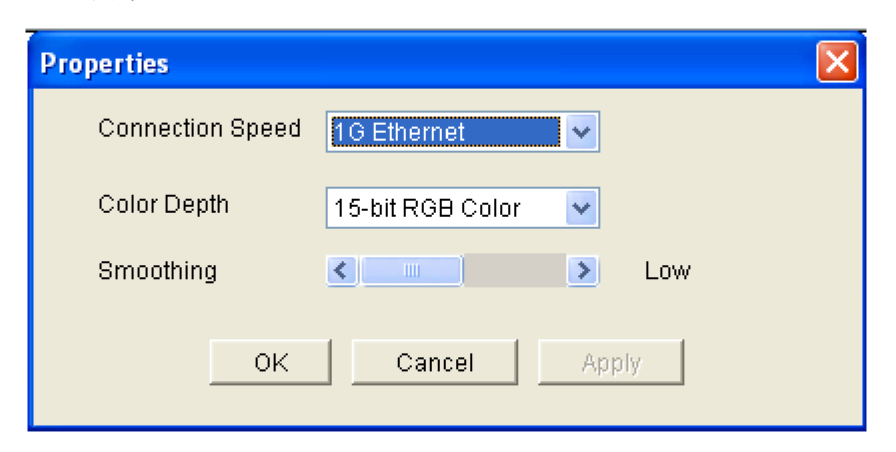
在不同的可用带宽环境下，动态视频压缩算法确保 KVM 控制台的可用性。设备不仅优化 LAN KVM 输出，还优化 WAN KVM 输出。对于任何带宽，这些设备还控制颜色深度，限制视频输出，从而在视频质量和系统响应应时间之间实现最佳平衡。

可以优化 Properties（属性）对话框上的参数，使其满足不同工作环境的要求。 在设置和保存连接属性时，把后续连接的连接属性保存到第二代设备上。

注意：KX II-101 的 VKC 使用的图标不同于其他 Dominion KX 产品的 VKC 使用的图标。参看 KX II-101 的 VKC 工具栏了解详情。

▶ 设置连接属性：

1. 选择 Connection（连接）> Properties（属性），或者单击工具栏上的 Connection Properties（连接属性）按钮 。打开 Properties（属性）对话框。



注意：KX II-101 不支持 1G Ethernet。

注意：KX II-101 的 VKC 使用的图标不同于其他 Dominion KX 产品的 VKC 使用的图标。参看 KX II-101 的 VKC 工具栏了解详情。

2. 在 Connection Speed（连接速度）下拉列表上选择连接速度。设备可以动态检测可用带宽，不限制带宽用量。但也可以根据带宽限制，调节此用量。
   - 自动
   - 1G Ethernet
   - 100 Mb Ethernet
   - 10 Mb Ethernet



- 1.5 Mb（最大 DSL/T1）
- 1 Mb（快速 DSL/T1）
- 512 Mb（中速 DSL/T1）
- 384 Mb（低速 DSL/T1）
- 256 Kb（电缆）
- 128 Kb（双 ISDN）
- 56 Kb（ISP 调制解调器）
- 33 Kb（快速调制解调器）
- 24 Kb（低速调制解调器）

注意这些设置对特定条件而言是优化设置，但不是准确速度。无论当前网络速度和编码设置如何，客户机和服务器始终尝试尽可能快地通过网络传输视频。但如何这些设置与实际环境相匹配，系统响应速度最快。

3. 在 Color Depth（颜色深度）下拉列表上选择颜色深度。设备可以动态适应给远程用户传输的颜色深度，使所有带宽的可用性最大化。
   - 15 位 RGB 彩色
   - 8 位 RGB 彩色
   - 4 位彩色
   - 4 位灰度
   - 3 位灰度
   - 2 位灰度
   - 黑白

重要说明：对大多数管理任务（服务器监视、重新配置等）而言，并不需要大多数显示卡支持的 24 位或 32 位真彩色。如果尝试发送这么高的颜色深度，会浪费网络带宽。

---

4. 用滑动条选择希望的 Smoothing（平滑度）（仅 15 位彩色模式）。平滑度确定屏幕区域与小色调变化组合成单一平滑色的尖锐程度。平滑可以减少视频噪声，从而改进目标服务器视频的外观。
5. 单击 OK（确定）按钮设置这些属性。



连接信息

获取 Virtual KVM Client 连接信息：

- 选择 Connection（连接）> Connection Info（连接信息）。打开 Connection Info（连接信息）窗口。

显示当前连接的下列信息：

- Device Name（设备名称）— 设备的名称。
- IP Address（IP 地址）— 设备的 IP 地址。
- Port（端口）— 访问目标设备所用的 KVM 通信 TCP/IP 端口。
- Data In/Second（数据输入/秒）— 数据输入速率。
- Data Out/Second（数据输出/秒）— 数据输出速率。
- Connect Time（连接时间）— 连接持续时间。
- FPS — 每秒传输的视频帧数。
- Horizontal Resolution（水平分辨率）— 屏幕水平分辨率。
- Vertical Resolution（垂直分辨率）— 屏幕垂直分辨率。
- Refresh Rate（刷新率）— 屏幕多久刷新一次。
- Protocol Version（协议版本）— RFB 协议版本。

复制这些信息：

- 单击 Copy to Clipboard（复制到剪贴板）。可以将这些信息粘贴到你选择的程序里。

键盘选项

键盘宏

键盘宏确保将针对目标服务器进行的击组合键发送到正确的目标服务器，并由该目标服务器解释。否则，Virtual KVM Client 所在的计算机（你的客户机 PC）可能会解释这些击组合键。

键盘宏存储在客户机 PC 上，是 PC 特定的。因此，如果使用另一台 PC，将看不到自己的键盘宏。此外，如果另一个人使用你的 PC，并用不同的用户名登录，他/她可以看到你的键盘宏，因为键盘宏是全局性的。

在 Virtual KVM Client 上创建的键盘宏可以在 MPC 上使用，反之亦然。但是，在 VKC 上创建的键盘宏不能在 AKC 或 MPC 上使用，反之亦然。



创建键盘宏

创建键盘宏：

1. 单击 Keyboard（键盘）> Keyboard Macros（键盘宏）。打开 Keyboard Macros（键盘宏）对话框。
2. 单击 Add（添加）按钮。打开 Add Keyboard Macros（添加键盘宏）对话框。
3. 在 Keyboard Macro Name（键盘宏名称）字段里输入键盘宏的名称。在创建键盘宏之后，Keyboard（键盘）菜单显示此名称。
4. 在 Hot-Key Combination（热组合键）字段里的下拉列表上选择键盘组合。这样，你可以用预定义的热键执行键盘宏。**可选**
5. 在 Keys to Press（要按的键）下拉列表上选择在执行该命令时，要用哪个键模拟相应的击键。按按键顺序选择这些键。在选择每个键之后，选择 Add Key（添加键）按钮。在选择每个键时，Macro Sequence（宏序列）字段显示该键，在每次选择之后自动添加 Release Key（释放键）命令。
6. 如要把 Send Text to Target（给目标发送文本）功能用于宏，单击 Construct Macro from Text（根据文本创建宏）按钮。
7. 例如创建一个宏，按左 Ctrl+Esc 关闭窗口。Macro Sequence（宏序列）字段显示的内容如下所示：

   Press Left Ctrl（按左 Ctrl）

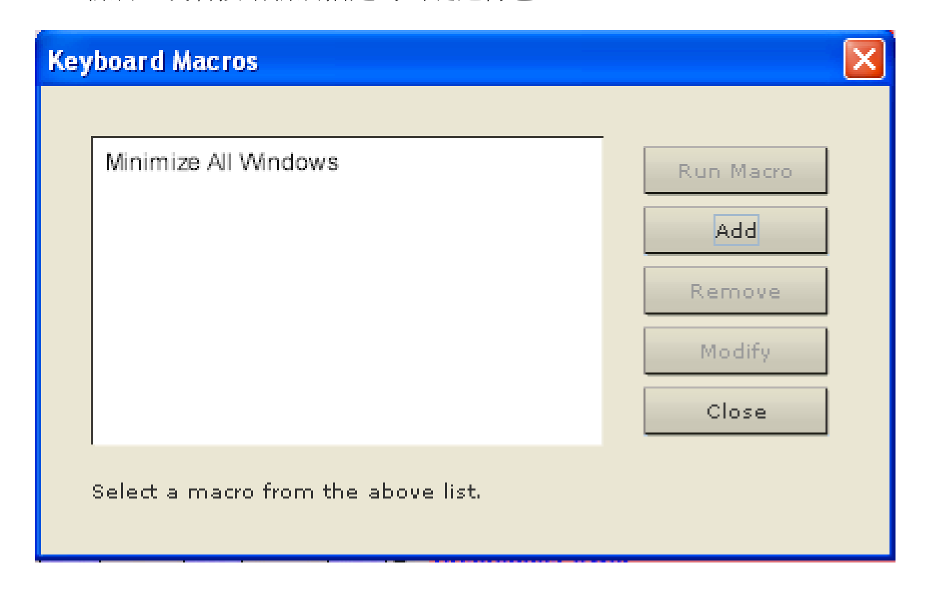
   Release Left Ctrl（释放左 Ctrl）

   Press Esc（按 Esc）

   Release Esc（释放 Esc）
8. 检查 Macro Sequence（宏序列）字段，确保宏序列定义正确无误。
   a. 如要删除序列中的一个步骤，选择该步骤，单击 Remove（删除）按钮。
   b. 如要更改序列中的步骤顺序，单击一个步骤，然后单击向上或向下箭头按钮，按需要重新排序步骤。
9. 单击 OK（确定）按钮保存宏。单击 Clear（清除）按钮清除所有字段，重新开始创建宏。在单击 OK（确定）按钮之后，打开 Keyboard Macros（键盘宏）对话框，列出新创建的键盘宏。



10. 单击 Close（关闭）按钮关闭 Keyboard Macros（键盘宏）对话框。应用程序的 Keyboard（键盘）菜单将显示该宏。在菜单上选择并运行新宏，或者按给新宏指定的击键运行它。



运行键盘宏

在创建键盘宏之后，可以用给它指定的键盘宏执行它，也可以在 Keyboard（键盘）菜单上选择并执行它。

通过菜单栏运行宏

在创建宏之后，Keyboard（键盘）菜单显示它。在 Keyboard（键盘）菜单上单击键盘宏，即可执行它。

用键盘组合运行宏

如果在创建宏时给它指定了键盘组合，可以按指定的击键执行宏。例如同是按 Ctrl+Alt+0 键使 Windows 目标服务器上的所有窗口最小化。

修改和删除键盘宏

► 修改宏：

1. 选择 Keyboard（键盘）> Keyboard Macros（键盘宏）。打开 Keyboard Macros（键盘宏）对话框。
2. 在列出的键盘宏中选择宏。
3. 单击 Modify（修改）。打开 Add/Edit Macro（添加/编辑宏）对话框。
4. 修改宏。
5. 单击 OK（确定）按钮。



▶ 删除宏：

1. 选择 Keyboard（键盘）> Keyboard Macros（键盘宏）。打开 Keyboard Macros（键盘宏）对话框。
2. 在列出的键盘宏中选择宏。
3. 单击 Remove（删除）按钮。宏被删除。

与刀片服务器机箱切换组合键相同的热键组合并不发送到这些机箱上的刀片服务器。

设置 CIM 键盘/鼠标选项

▶ 访问 DCIM-USBG2 设置菜单：

1. 将鼠标放在 Note Pad（Windows®操作系统）或类似编辑器窗口上。
2. 选择 Set CIM Keyboard/Mouse（设置 CIM 键盘/鼠标）选项。这相当于将左 Ctrl 和 Num Lock 信号发送到目标服务器。然后显示 CIM 设置菜单选项。
3. 设置语言和鼠标设置。
4. 退出菜单，返回正常 CIM 功能。

视频属性

刷新屏幕

Refresh Screen（刷新屏幕）命令强制刷新显示屏幕。可以采用几种方法刷新视频设置：

- Refresh Screen（刷新屏幕）命令强制刷新显示屏幕。
- Auto-sense Video Settings（自动检测视频设置）命令自动检测目标服务器的视频设置。
- Calibrate Color（校准颜色）命令校准视频，从而增强正在显示的颜色。

此外，可以用 Video Settings（视频设置）命令人工调节设置。

注意：KX II-101 的 VKC 使用的图标不同于其他 Dominion KX 产品的 VKC 使用的图标。参看 KX II-101 的 VKC 工具栏了解详情。

▶ 执行下列操作之一刷新视频设置：

- 选择 Video（视频）> Refresh Screen（刷新屏幕），或者单击工具栏上的 Refresh Screen（刷新屏幕）按钮。



自动检测视频设置

Auto-sense Video Settings（自动检测视频设置）命令强制重新检测视频设置（分辨率和刷新率），并刷新显示屏幕。

注意：KX II-101 的 VKC 使用的图标不同于其他 Dominion KX 产品的 VKC 使用的图标。参看 KX II-101 的 VKC 工具栏了解详情。

▶ 执行下列操作自动检测视频设置：

- 选择 Video（视频）> Auto-sense Video Settings（自动检测视频设置），或者单击工具栏上的 Auto-Sense Video Settings（自动检测视频设置）按钮。显示一条消息，说明正在进行自动调节。

校准颜色

用 Calibrate Color（校准颜色）命令优化传输的视频图像的色阶（色调、亮度和饱和度）。不同的目标服务器使用不同的颜色设置。

注意：Calibrate Color（校准颜色）命令只应用于当前连接。

注意：KX II-101 支持颜色较准。

▶ 执行下列操作校准颜色：

- 选择 Video（视频）> Calibrate Color（校准颜色），或者单击工具栏上的 Calibrate Color（校准颜色）按钮。目标服务器屏幕反映颜色校准。

调节视频设置

用 Video Settings（视频设置）命令人工调节视频设置。

▶ 更改视频设置：

1. 选择 Video（视频）> Video Settings（视频设置），或者单击工具栏上的 Video Settings（视频设置）按钮，打开 Video Settings（视频设置）对话框。
2. 按需要调节下列设置。在调节设置时，立刻可以看到调节效果：
   a. Noise Filter（噪声过滤器）

设备可以过滤来自显示卡的视频输出的电气干扰。此功能可以优化图像质量，减少所需的带宽。只有在与相邻像素相比存在很大的色调变化时，较高的设置才传输可变像素。但如果将阈值设置得太高，可能会无意间将期望的屏幕变化过滤掉。
如果设置太低，要传输大多数像素变化。如果将此阈值设置得太小，可能会提高带宽用量。

b. PLL 设置 (PLL Settings)：

Clock（时钟）— 控制显示屏幕显示视频像素的速度。在更改时钟设置时，视频图像会水平伸展或收缩。建议你使用奇数设置。在大多数情况下，不应更改此设置，因为自动检测功能的检测结果通常很精准。

Phase（相位）— 相位值在 0-31 之间，在达到 31 之后返回 0。当活动目标服务器显示最佳视频图像时，即停止调节相位值。

c. Brightness（亮度）：用此设置调节目标服务器显示器的亮度。

d. Brightness Red（亮度红色）— 控制目标服务器显示器的红色信号的亮度。

e. Brightness Green（亮度绿色）— 控制绿色信号的亮度。

f. Brightness Blue（亮度蓝色）— 控制蓝色信号的亮度。

g. Contrast Red（对比度红色）— 控制红色信号对比度。

h. Contrast Green（对比度绿色）— 控制绿色信号。

i. Contrast Blue（对比度蓝色）— 控制蓝色信号。

如果视频图像看上去非常模糊或不聚焦，可以调节时钟设置和相位设置，直到活动目标服务器显示质量较高的图像为止。

警告：在更改时钟设置和相位设置时务必小心。更改时钟设置和相位设置可能会导致屏幕不显示视频，或者视频变形，可能无法返回此前的状态。在进行任何更改之前，请联系 Raritan 技术支持部门。

---

j. Horizontal Offset（水平偏移）— 控制目标服务器显示器在你的监视器上的水平位置。

k. Vertical Offset（垂直偏移）— 控制目标服务器显示器在你的监视器上的垂直位置。

3. 选择 Auto Color Calibration（自动颜色校准）启用此功能。

4. 选择视频检测模式：

   - Best possible video mode（最佳视频模式）

   在切换目标服务器或目标分辨率时，设备执行全面自动检测进程。选择此选项校准视频，使视频质量最佳。

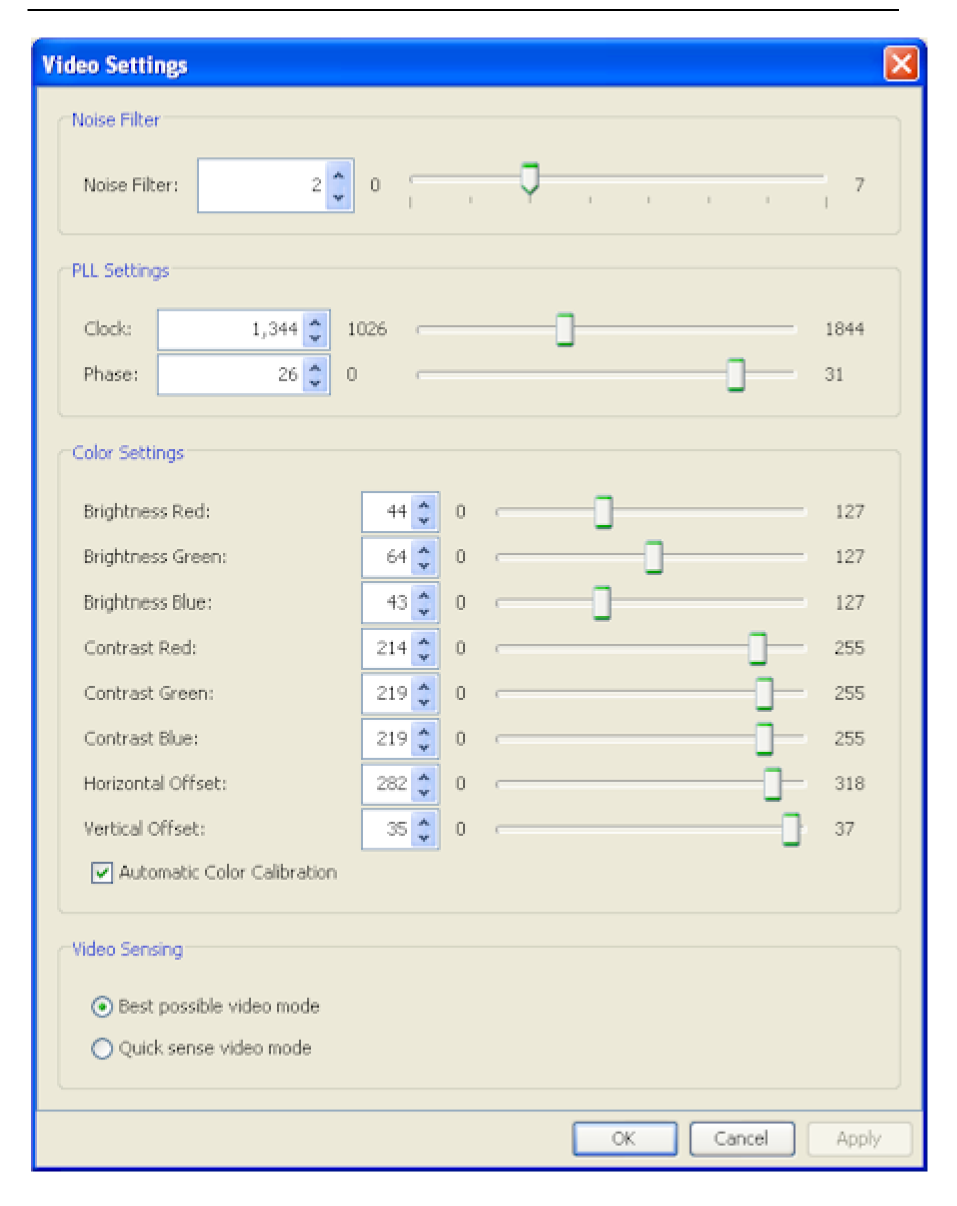


- Quick sense video mode（快速检测视频模式）

  在选择此选项之后，设备使用快速视频自动检测，迅速显示目标服务器的视频。在目标服务器重新启动之后马上进入其 BIOS 配置时，此选项尤其有用。

5. 单击 OK（确定）按钮应用设置，并关闭对话框。单击 Apply（应用）按钮应用设置，但不关闭对话框。

注意：在某些 Sun 背景屏幕上，例如有黑边的屏幕，某些 Sun 服务器可能不精确居中。使用另一个背景，或者在屏幕左上角放一个浅色图标。





注意：KX II-101 的 VKC 使用的图标不同于其他 Dominion KX 产品的 VKC 使用的图标。参看 KX II-101 的 VKC 工具栏了解详情。

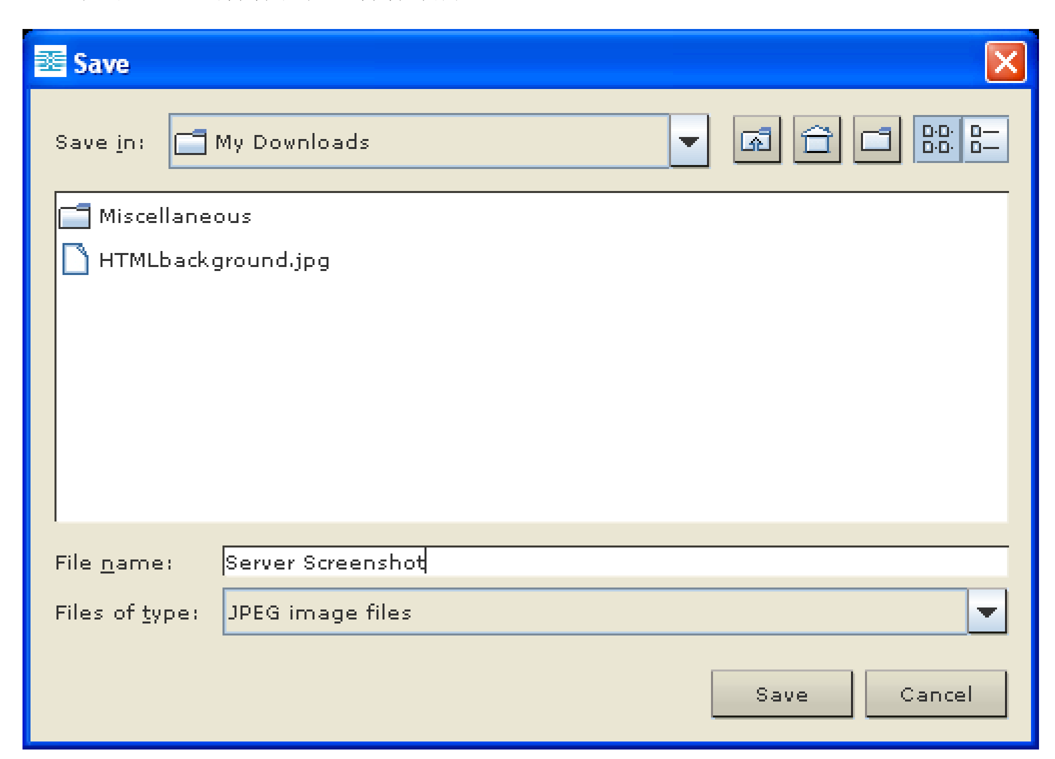
使用目标服务器截屏

可以用 Screenshot from Target server（目标服务器截屏）命令截取目标服务器屏幕。可以采用 bitmap、JPEG 或 PNG 格式把此截屏保存到所选的文件位置。

注意：KX II-101 不支持目标服务器截屏功能。

截取目标服务器屏幕：

1. 选择 Video（视频）> Screenshot from Target（目标服务器截屏），或者单击工具栏上的 Screenshot from Target（目标服务器截屏）按钮 。
2. 在 Save（保存）对话框上选择文件保存位置，输入文件名，在 Files of type（文件类型）下拉列表上选择文件格式。
3. 单击 Save（保存）按钮保存截屏。





更改最大刷新速率

如果目标服务器上的显示卡使用定制软件，而你通过 MPC 或 VKC 访问目标服务器，可能必须更改监视器的最大刷新速率，刷新速率才会在目标服务器上生效。

▶ **调节监视器刷新速率：**

1. 在 Windows® 上选择 Display Properties（显示属性）> Settings（设置）> Advanced（高级），打开 Plug and Play（即插即用）对话框。
2. 单击 Monitor（监视器）选项卡。
3. 把 Screen refresh rate（屏幕刷新速率）设置为大于 100Hz 的任何速率。
4. 单击 OK（确定）按钮，再单击 OK（确定）按钮应用设置。

鼠标选项

在控制目标服务器时，Remote Console 显示两个鼠标光标：一个属于客户机工作站，另一个属于目标服务器。

你既可以在单鼠标模式下操作，也可以在双鼠标模式下操作。在双鼠标模式下，假如适当配置此选项，两个鼠标光标重叠。

在有两个鼠标光标时，设备有几种鼠标模式：

- 绝对（鼠标同步）
- 智能（鼠标模式）
- 标准（鼠标模式）

鼠标指针同步

在远程查看使用鼠标的目标服务器时，你会看到两个鼠标光标：一个是远程客户机工作站的鼠标光标，另一个是目标服务器的鼠标光标。当鼠标指针位于 Virtual KVM Client 目标服务器窗口内时，鼠标移动和单击操作直接发送到相连的目标服务器。在鼠标移动时，由于鼠标加速度设置的缘故，客户机鼠标指针相对于目标服务器鼠标指针稍稍提前一点。

在快速 LAN 连接上，你可能要禁用 Virtual KVM Client 鼠标指针，只看到目标服务器的鼠标指针。可以在两种模式（单鼠标模式和双鼠标模式）之间来回切换。

注意：KX II-101 的 VKC 使用的图标不同于其他 Dominion KX 产品的 VKC 使用的图标。参看 KX II-101 的 VKC 工具栏了解详情。

鼠标同步提示

在配置鼠标同步时，务必遵循下列步骤：

1. 确定选择的视频分辨率和刷新速率在此设备支持的范围内。Virtual KVM Client Connection Info（连接信息）对话框显示此设备看到的实际值。
2. 确定电缆长度是否在选择的视频分辨率要求的指定范围内。
3. 确定在安装过程中是否正确配置了鼠标和视频。
4. 单击 Virtual KVM Client 自动检测按钮，强制进行自动检测。
5. 如果这不能改善鼠标同步（Linux、UNIX 和 Solaris KVM 目标服务器）：
   a. 打开终端窗口。
   b. 输入 `xset mouse 1 1` 命令。
   c. 关闭终端窗口。
6. 单击 Virtual KVM Client 鼠标同步按钮  。



智能鼠标模式附加说明

- 确保屏幕左上角没有图标或应用程序，因为这是同步例程执行位置。
- 切勿使用动画鼠标。
- 在 KVM 目标服务器上禁用活动桌面。

同步鼠标

在双鼠标模式下，Synchronize Mouse（同步鼠标）命令强制目标服务器鼠标指针与 Virtual KVM Client 鼠标指针重叠。

▶ 执行下列操作之一同步鼠标：

- 选择 Mouse（鼠标）> Synchronize Mouse（同步鼠标），或者单击工具栏上的 Synchronize Mouse（同步鼠标）按钮 。

标准鼠标模式

标准鼠标模式使用标准鼠标同步算法，使用相对鼠标位置。为了让客户机鼠标和服务器鼠标保持同步，标准鼠标模式要求禁用鼠标加速度，正确设置其他鼠标参数。标准鼠标模式是默认模式。

▶ 进入标准鼠标模式：

- 选择 Mouse（鼠标）> Standard（标准）。

智能鼠标模式

在智能鼠标模式下，设备可以检测目标服务器鼠标设置，相应地同步鼠标光标，在目标服务器上启用鼠标加速度。在此模式下，鼠标光标不跳到屏幕左上角计算加速度。为了让此模式正常工作，必须满足某些条件。

进入智能鼠标模式：

- 选择 Mouse（鼠标）> Intelligent（智能）。

智能鼠标同步条件

在鼠标闲置时，Mouse（鼠标）菜单上的 Intelligent Mouse Synchronization（智能鼠标同步）命令自动同步鼠标指针。为了让此模式正常工作，必须满足下列条件：

- 应该在目标服务器上禁用活动桌面。
- 目标服务器页面左上角不应该有窗口。
- 目标服务器页面左上角不应该有动画背景。
- 目标服务器鼠标光标的形状应该是正常形状，不应是动画光标。
- 目标服务器鼠标速度不应设置为太小或太大的值。
- 应该禁用 Enhanced pointer precision（增强指针精度）或 Snap mouse to default button in dialogs（在对话框上捕捉鼠标至默认按钮）等高级鼠标属性。
- 在 Video Settings（视频设置）窗口上选择 Best Possible Video Mode（最佳视频模式）。
- 目标服务器视频的边沿应该清晰可见(即当你滚到目标服务器视频图像边沿时，目标服务器桌面和远程 KVM 控制台窗口之间的黑边应该是可见的）。
- 在使用智能鼠标同步功能时，桌面左上角的文件图标或文件夹图标可能会导致此功能不能正常工作。为了避免此功能出任何问题，Raritan 建议你不要将任何文件图标或文件夹图标放在桌面左上角。

在自动检测目标服务器视频之后，单击工具栏上的 Synchronize Mouse（同步鼠标）按钮人工开始鼠标同步。在目标服务器分辨率变化时，如果鼠标指针开始彼此不同步，也可以这么做。

如果智能鼠标同步失败，此模式将切换回标准鼠标同步模式。

请注意在不同的目标服务器操作系统上，鼠标配置会有差异。参看操作系统指南了解详情。同时还要注意，智能鼠标同步对 Unix 目标服务器无效。



绝对鼠标模式

在此模式下，用绝对坐标使客户机光标和目标服务器光标保持同步，即使目标服务器鼠标设置为不同的加速度或速度也没有关系。有 USB 端口的服务器支持此模式。

▶ 进入绝对鼠标模式：

- 选择 Mouse（鼠标）> Absolute（绝对）。

注意：绝对鼠标设置要求 USB 目标系统，是给 KX II-101 建议的鼠标设置。

注意：绝对鼠标同步仅用于支持虚拟媒体的 USB CIM（D2CIM-VUSB 和 D2CIM-DVUSB）。

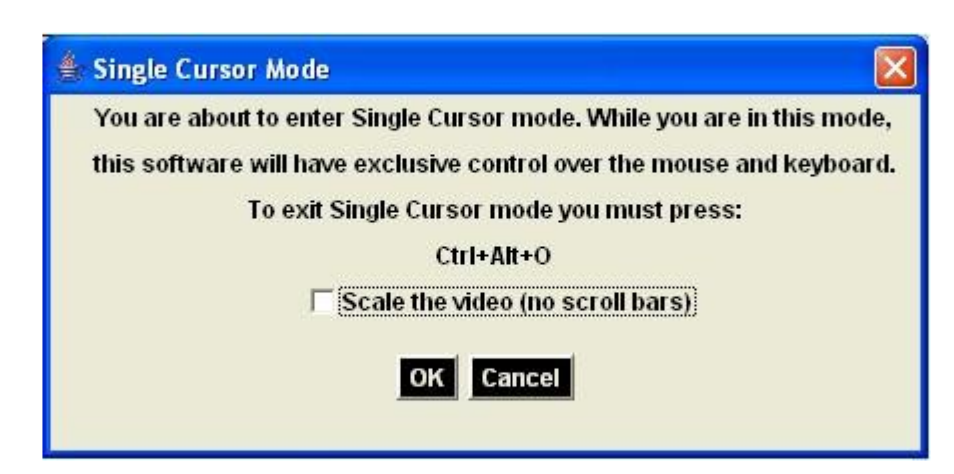
单鼠标光标

单鼠标模式只使用目标服务器鼠标光标，屏幕不再显示本地鼠标指针。在单鼠标模式下，不能使用 Synchronize Mouse（同步鼠标）命令（不必同步一个鼠标光标）。

注意：KX II-101 的 VKC 使用的图标不同于其他 Dominion KX 产品的 VKC 使用的图标。参看 KX II-101 的 VKC 工具栏了解详情。

▶ 执行下列操作进入单鼠标模式：

1. 选择 Mouse（鼠标）> Single Mouse Cursor（单鼠标光标）。
2. 单击工具栏上的 Single/Double Mouse Cursor（单/双鼠标光标）按钮 。



退出单鼠标模式：

1. 按键盘上的 Ctrl+Alt+O 退出单鼠标模式。

VKC 虚拟媒体

参看虚拟媒体一章，详细了解如何设置和使用虚拟媒体。

智能卡（VKC、AKC 和 MPC）

如果使用 KX II 2.1.10 或更高版本，可以在目标服务器上安装智能卡读卡器支持智能卡验证和相关应用。 参看***支持的和不支持的智能卡读卡器*** (p. 270)，了解支持的智能卡、智能卡读卡器和其他系统要求清单。

在远程访问服务器时，可以选择所连接的智能卡读卡器，把它安装在服务器上。智能卡验证用于与目标服务器进行验证，并非用于登录目标服务器。因此，更改智能卡 PIN 和证书不需要更新设备帐号。 在目标服务器上安装读卡器之后，可以像使用直接连接的读卡器一样使用服务器上的读卡器和智能卡。在取下智能卡或智能卡读卡器之后，根据在目标服务器操作系统上设置的取卡策略，系统要么锁定用户会话，要么不让你退出系统。在因关闭 KVM 会话或切换到新目标服务器而终止 KVM 会话之后，自动把智能卡读卡器从目标服务器上卸载掉。

在设备上启用 PC-Share（PC 共享）模式之后，多个用户可以同时访问一台目标服务器。但如果目标服务器连接智能卡读卡器，无论是否选择了 PC-Share（PC 共享）模式，设备都将执行隐私保护策略。此外，如果你加入目标服务器的共享会话，将禁止安装智能卡读卡器，直到可以独占访问目标服务器为止。

在与目标服务器建立 KVM 会话之后，可以使用 Virtual KVM Client 和 Multi-Platform Client 上的 Smart Card（智能卡）菜单和按钮。在打开 Smart Card（智能卡）菜单或选择智能卡按钮之后，显示检测到的、与远程客户机相连的智能卡读卡器。可以在此对话框上连接其他智能卡读卡器，刷新与目标服务器相连的智能卡读卡器的列表，断开智能卡读卡器。还可以取出或插入智能卡。可以用此功能通知目标服务器操作系统，必须取出/重新插入智能卡才能显示相应的登录对话框。可以用此功能给一台目标服务器发送通知，但不影响其他 KVM 活动会话。

安装智能卡读卡器：

1. 单击 Smart Card（智能卡）菜单，选择 Smart Card Reader（智能卡读卡器）。也可以单击工具栏上的 Smart Card（智能卡）按钮 。
2. 在 Select Smart Card Reader（选择智能卡读卡器）对话框上选择智能卡读卡器。
3. 单击 Mount（安装）按钮。

4. A progress dialog will open.选择 Mount selected card reader automatically on connection to targets（在连接目标服务器时自动安装选择的读卡器）复选框，在下次连接服务器时自动安装智能卡读卡器。单击 OK（确定）按钮开始安装过程。

在 Select Smart Card Reader（选择智能卡读卡器）对话框上更新智能卡：

- 如果客户机 PC 连接新智能卡读卡器，单击 Refresh List（刷新列表）。

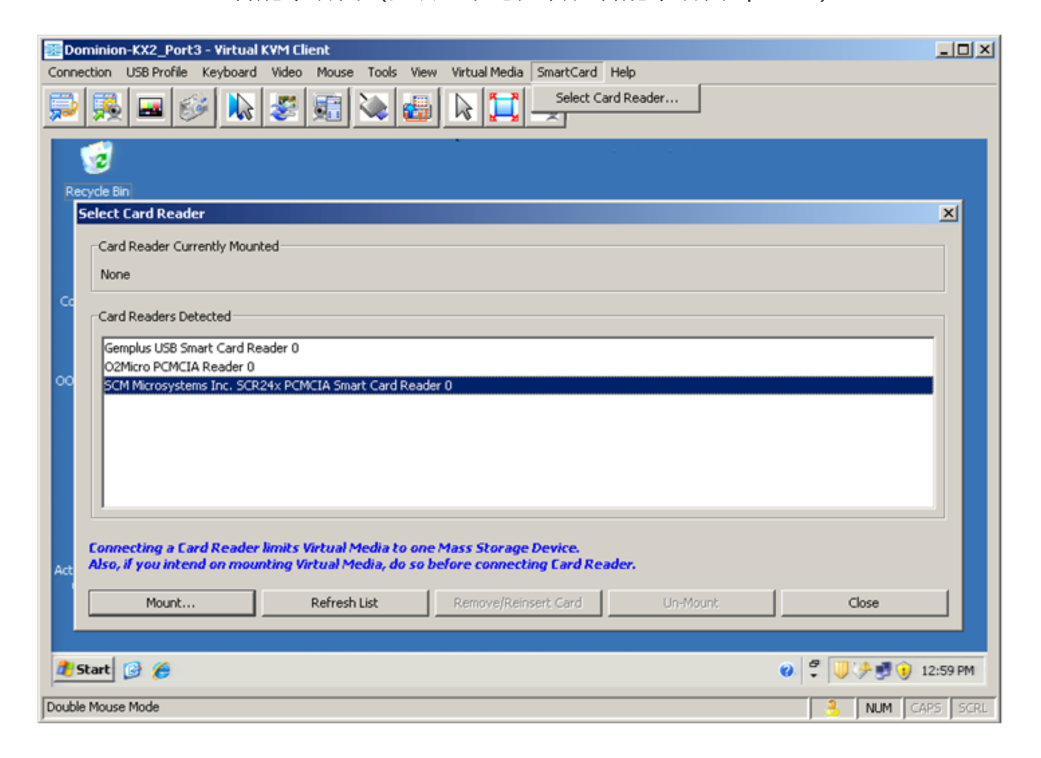
给目标服务器发送智能卡取出和重新插入通知：

- 单击当前安装的智能卡读卡器，单击 Remove/Reinsert（取出/重新插入）按钮。

卸载智能卡读卡器：

- 选择要卸载的智能卡读卡器，单击 Unmount（卸载）按钮。

还可以在 Local Console 上安装智能卡读卡器。参看 KX II 帮助中的 **Local Console 智能卡访问** (参看 "**本地控制台智能卡访问**" p. 237)。





工具选项

可以在 Tools（工具）菜单上指定 Virtual KVM Client 使用的某些选项，包括日志记录，设置键盘类型，给现有的全屏模式和单光标模式定义热键。

▶ 设置工具选项：

1. 选择 Tools（工具）> Options（选项）。打开 Options（选项）对话框。
2. 只有在技术支持人员的指导下，才能选择 Enable Logging（启用日志）复选框。此选项在主目录下创建一个日志文件。
3. 在 Keyboard Type（键盘类型）下拉列表上选择键盘类型（如有必要）。选项包括：
   - US/International（美国英文/国际）
   - French (France)（法文[法国]）
   - German (Germany)（德文[德国]）
   - Japanese（日文）
   - United Kingdom（英国英文）
   - Korean (Korea)（朝鲜文[韩国]）
   - Belgian (Belgium)（比利时）
   - Norwegian (Norway)（挪威文[挪威]）
   - Portuguese（葡萄文[葡萄牙]）
   - Danish (Denmark)（丹麦文[丹麦]）
   - Swedish (Sweden)（瑞典文[瑞典]）
   - German (Switzerland)（德文[瑞士]）
   - Hungarian (Hungary)（匈牙利文[匈牙利]）
   - Spanish (Spain)（西班牙文[西班牙]）
   - Italian (Italy)（意大利文[意大利]）
   - Slovenian（斯洛文尼亚文）
   - Translation: French - US（翻译：法文 - 美国英文）
   - Translation: French - US International（翻译：法文 - 美国国际英文）

注意：在 AKC 里，键盘类型默认本地客户机，所以此选项不适用。



4. 退出全屏模式 — 热键。在进入全屏模式时，全屏显示目标服务器，使用与目标服务器相同的分辨率。这是退出此模式所用的热键。
5. 退出单光标模式 — 热键。在进入单光标模式时，只显示目标服务器鼠标光标。这是退出单光标模式、返回客户机鼠标光标所用的热键。单击 OK（确定）按钮。

客户机启动设置

KX II 用户还可以配置客户机启动设置，便于你给 KVM 会话定义屏幕大小。

6. 选择 Client Launch Settings（客户机启动设置）选项卡。
   a. 配置目标窗口设置：
   - 选择 Standard - sized to target Resolution（标准调节目标分辨率大小），用目标窗口的当前分辨率打开窗口。如果目标分辨率大于客户机分辨率，目标窗口尽可能覆盖整个窗口，并显示滚动条（如有必要）。
   - 选择 Full Screen（全屏），按全屏模式打开打开窗口。

   a. 配置要在哪个监视器上打开目标查看器：
   - 如果要使用与客户机（例如网络浏览器或小程序）相同的应用程序显示方式启动目标查看器，选择 Monitor Client Was Launched from（监视器客户机旧启动方式）。
7. 选择 Select From Detected Monitors（在检测到的监视器中选择），在应用程序当前检测到的目标监视器列表上选择监视器。如果再也检测不到此前选择的监视器，显示 Currently Selected Monitor Not Detected（检测不到当前选择的监视器）。
8. 单击 OK（确定）按钮。

键盘限制

斯洛文尼亚文键盘

由于 JRE 限制，斯洛文尼亚文键盘上的 < 键不起作用。

Linux 语言配置

由于 Linux 运行的 Sun JRE 在给用 System Preferences（系统首选项）配置的外文键盘生成正确的键事件时有问题，Raritan 建议你用下表所述的方法配置外文键盘。

语言	配置方法
美国英语/国际	默认值
法文	Keyboard Indicator（键盘指示器）
德文	System Settings（系统设置）(Control Center[控制中



语言	配置方法
	心])
日文	System Settings（系统设置）(Control Center[控制中心])
英国英语	System Settings（系统设置）(Control Center[控制中心])
朝鲜文	System Settings（系统设置）(Control Center[控制中心])
比利时	Keyboard Indicator（键盘指示器）
挪威文	Keyboard Indicator（键盘指示器）
丹麦文	Keyboard Indicator（键盘指示器）
瑞典文	Keyboard Indicator（键盘指示器）
匈牙利文	System Settings（系统设置）(Control Center[控制中心])
西班牙文	System Settings（系统设置）(Control Center[控制中心])
意大利文	System Settings（系统设置）(Control Center[控制中心])
斯洛文尼亚文	System Settings（系统设置）(Control Center[控制中心])
葡萄牙文	System Settings（系统设置）(Control Center[控制中心])

注意：在使用 Gnome 作为桌面环境的 Linux 系统上，应该使用 Keyboard Indicator（键盘指示器）。



视图选项

视图工具栏

可以在显示或不显示工具栏的情况下使用 Virtual KVM Client。

切换工具栏显示（打开和关闭）：

- 选择 View（视图）> View Toolbar（视图工具栏）。

缩放比例

缩放目标窗口，可以看到目标服务器窗口的整个内容。此功能能增大或缩小目标视频大小，使之适合 Virtual KVM Client 窗口大小，并保持长宽比不变，即使你不使用滚动条也能看到整个目标服务器桌面。

切换缩放（打开和关闭）：

- 选择 View（视图）> Scaling（缩放）。

目标屏幕分辨率

在进入全屏模式时，全屏显示目标服务器，使用与目标服务器相同的分辨率。在 Options（选项）对话框上指定退出此模式所用的热键（默认设置是 Ctrl+Alt+M）。在全屏模式中，把鼠标移动到屏幕顶部，将显示全屏模式菜单栏。

进入全屏模式：

- 选择 View（视图）> Full Screen（全屏）。

退出全屏模式：

- 按在 Tools Options（工具选项）对话框上配置的热键。默认设置是 Ctrl+Alt+M。在 AKC 里，把鼠标移动到屏幕顶部显示隐藏的菜单栏，选择 Connection/Exit（连接/退出）。

如果希望始终在全屏模式下访问目标服务器，可以把全屏模式设置为默认模式。

把全屏模式设置为默认模式：

1. 单击 Tools（工具）> Options（选项），打开 Options（选项）对话框。
2. 单击 Enable Launch in Full Screen Mode（启用在全屏模式下启动）图标，单击 OK（确定）按钮。



帮助选项

关于 Raritan Virtual KVM Client

当你需要 Raritan 技术支持部门的协助时，此菜单命令提供 Virtual KVM Client 版本信息。

► 获取版本信息：

1. 选择 Help（帮助）> About Raritan Virtual KVM Client（关于 Raritan Virtual KVM Client）。
2. 用 Copy to Clipboard（复制到剪贴板）按钮将对话框上的信息复制到剪贴板文件里，以便稍后在联系支持人员时访问（如有必要）。

Active KVM Client (AKC)

概述

建立在 Microsoft Windows .NET 之上的 Active KVM Client (AKC) 可用于 KX II 2.2（或更高版本），支持所有 KX II 设备，但目前尚未支持 KX2-101 和 KSX2 设备。AKC 建立在 Microsoft Windows .NET 技术之上，允许用户在不使用 Java Runtime Environment (JRE) 的 Windows 环境下运行客户机，而运行 Raritan Virtual KVM 和 Multi-Platform 客户机需要 Java Runtime Environment (JRE)。AKC 还可与 CC-SG 一起工作。

AKC 和 VKC 具有相似的功能，只有下列各项除外：

- 最低系统要求
- 支持的操作系统和浏览器
- VKC 不使用在 AKC 里创建的键盘宏

参看 ***Virtual KVM Client*** (p. 52) 一节，了解如何使用此应用程序的功能。如果 AKC 功能和 VKC 功能有差异，本主题加以说明。

同时参看***启用直接端口访问*** (p. 141)和***启用 AKC 下载服务器证书验证*** (p. 142),了解如何配置 AKC。

注意：如果使用 AKC 进行直接端口访问，必须针对要访问的每个目标服务器打开一个新浏览器窗口或新书签。当前正在访问一台目标服务器，如果在同一个浏览器窗口或浏览器书签上输入 LDAP URL 访问另一台目标服务器，不能建立连接，可能显示错误消息。



AKC 支持的操作系统和浏览器

.NET Framework

AKC 需要 Windows .NET® v3.5，可以使用已安装的 v3.5 和 v4.0。

操作系统

在 Internet Explorer® 上启动 AKC 或作为独立应用程序启动 AKC 时，可以通过 KX II 2.2（或更高版本）访问目标服务器。AKC 兼容运行 .NET Framework 3.5 的下列平台：

- Windows XP® 操作系统
- Windows Vista® 操作系统（64 位）
- Windows 7® 操作系统（64 位）

注意：如果打开 WINDOWS PC FIPS，并用 AKC 和智能卡访问目标服务器，必须使用 Windows 7。

由于运行 AKC 需要 .NET，如果没有安装 .NET，或者安装了不支持的 .NET 版本，系统显示一条消息，告诉你如何检查 .NET 版本。

浏览器

- Internet Explorer 6 或更高版本

如果尝试在除 IE 6 或更高版本之外的浏览器上打开 AKC，系统显示一条消息，告诉你如何检查浏览器并切换到 Internet Explorer。

使用 AKC 的前提

为了使用 AKC：

- 确保当前不阻止来自正在访问的设备的 IP 地址的 cookies。
- Windows Vista、Windows 7 和 Windows 2008 服务器用户应该确保正在访问的设备的 IP 地址位于浏览器的 Trusted Sites Zone（信任网站区域），在访问设备时不在 Protected Mode（保护模式）下。

启用 AKC 下载服务器证书验证

如果 KX II（或 CC-SG）管理员启用了 Enable AKC Download Server Certificate Validation（启用 AKC 下载服务器证书验证）选项：

- 管理员必须把有效证书上载到 KX II 上，或者在 KX II 上创建一个自签名证书。证书必须有有效主机名。
- 每个用户必须把 CA 证书（或自签名证书）添加到浏览器的 Trusted Root CA 仓库。

在 CC-SG Admin Client 上启动 AKC 时，必须有 JRE™ 1.6.0_10 或更高版本。



Ch 4 电源条（机架式 PDU）接口控制

在本章内

概述

Dominion KX II 允许你控制通过 D2CIM-PWR 与 Dominion KX II 相连的 Raritan PX 和 RPC 系列电源条接口。

在设置 PX 或 RPC 系列电源条并把它们连接到 Dominion KX II 之后，可以在 Dominion KX II 界面的 Powerstrip（电源条）页上控制电源条及其接口。单击页面顶部的 Power（电源）菜单，即可访问本页。

Powerstrip（电源条）页显示与用户有适当端口访问权的 Dominion KX II 相连的电源条。在级联配置情况下，Powerstrip（电源条）页同时显示与用户有适当端口访问权的基础 Dominion KX II 和级联 Dominion KX II 相连的电源条。

注意：参看 ***Dominion PX 用户指南****了解如何设置 PX。*

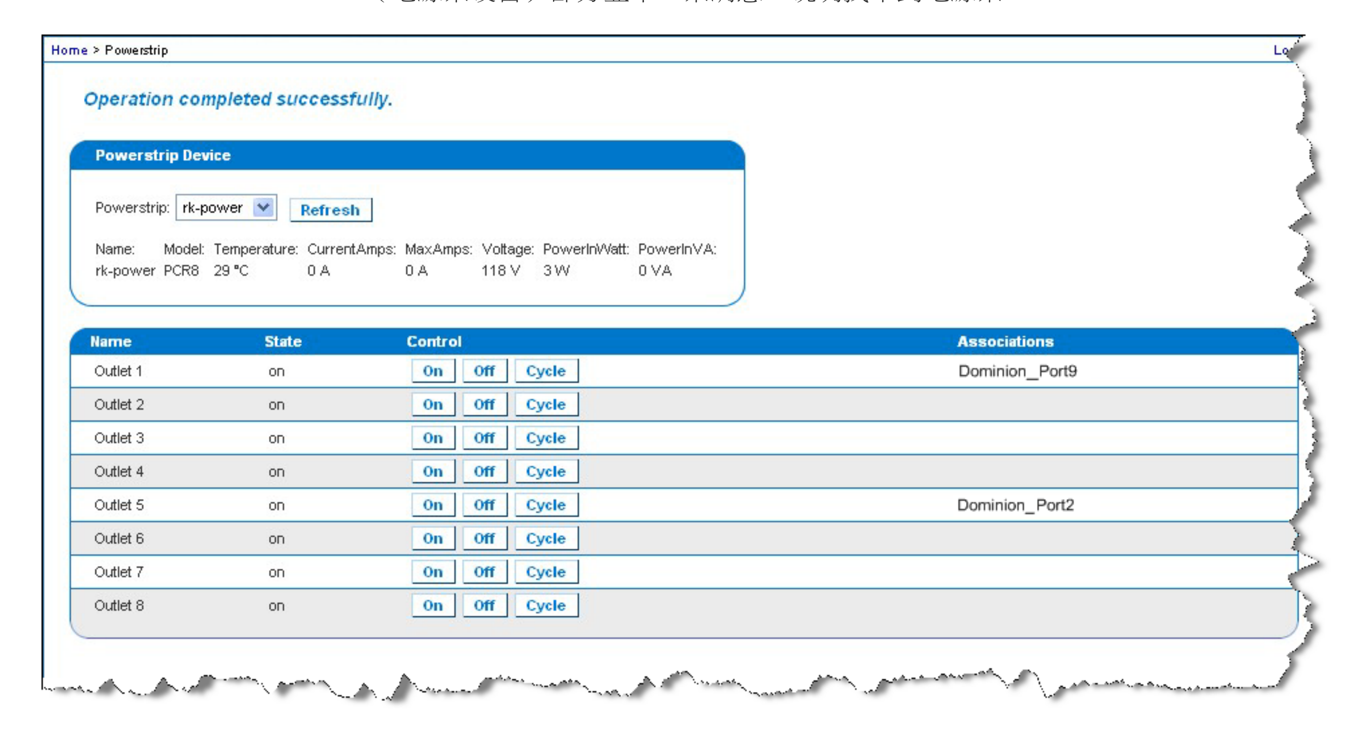
可以在 Powerstrip（电源条）页上给电源接口通电、断电和重新通电。还可以查看下列电源条信息和接口信息：

- 电源条设备信息：
  - Name（名称）
  - 型号
  - 温度
  - Current Amps（电流[安培]）
  - Maximum Amps（最大电流）
  - Voltage（电压）
  - Power in Watts（功率[瓦]）
  - Power in Volts Ampere（功率[伏安]）
- 电源接口显示信息：
  - Name（名称）— 在配置接口时给它指定的名称。
  - State（状态）— 电源接口的开或关状态。
  - Control（控制）— 给电源接口通电、断电或重新通电。



- Association（关联）— 与电源接口关联的端口。

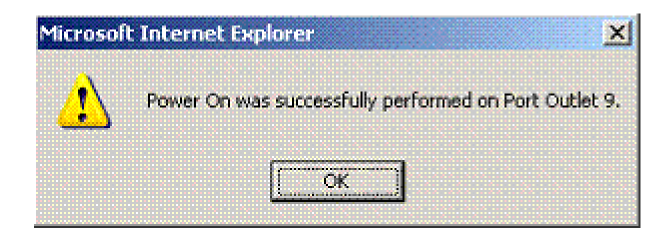
最初打开 Powerstrip（电源条）页时，Powerstrip（电源条）下拉列表显示当前与 Dominion KX II 相连的电源条。此外，还显示有关当前选择的电源条的信息。如果没有任何电源条连接 Dominion KX II，本页的 Powerstrip Device（电源条设备）部分显示一条消息，说明找不到电源条。



接通/断开接口电源和重新通电

▶ 接通接口电源：

1. 单击 Power（电源）菜单访问 Powerstrip（电源条）页。
2. 在 Powerstrip（电源条）下拉列表上选择要通电的 PX 电源条。
3. 单击 Refresh（刷新）按钮查看电源控制。
4. 单击 On（开）。

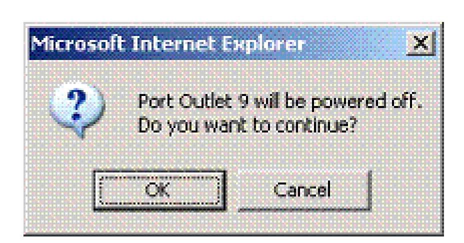




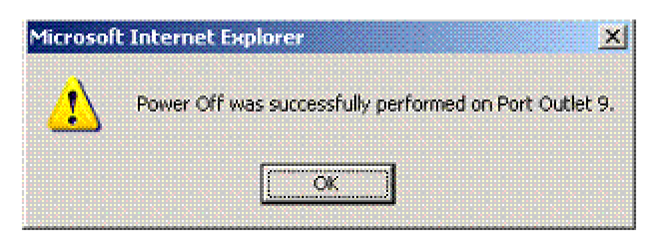
5. 单击 OK（确定）按钮关闭 Power On（通电）确认对话框。接通接口电源，其状态为 on（开）。

断开接口电源：

1. 单击 Off（关）。
2. 单击 Power Off（断电）对话框上的 OK（确定）按钮。

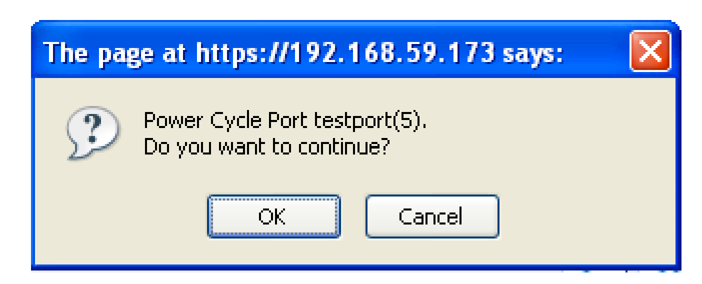


3. 单击 Power Off（断电）确认对话框上的 OK（确定）按钮。断开接口电源，其状态为 off（关）。



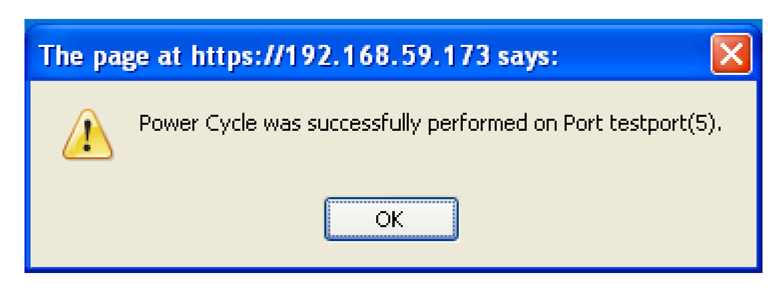
给电源接口重新通电：

1. 单击 Cycle（重新通电）按钮。打开 Power Cycle Port（给端口重新通电）对话框。





2. 单击 OK（确定）按钮。给电源接口重新通电（注意这可能需要几秒钟时间）。



3. 在重新通电结束之后，打开对话框。单击 OK（确定）按钮关闭对话框。



Ch 5 虚拟媒体

在本章内



概述

虚拟媒体允许 KVM 目标服务器通过客户机 PC 和网络文件服务器远程访问介质，从而扩展了 KVM 功能。通过这种功能，在客户机 PC 和网络文件服务器上安装的介质本质上是以虚拟方式安装在目标服务器上。随后，目标服务器可以读写这些介质，就像读写与目标服务器直接相连的介质一样。除了通过虚拟媒体支持数据文件，虚拟媒体还通过 USB 连接支持文件。

虚拟媒体可以包括内置和 USB 安装的 CD 驱动器、DVD 驱动器、USB 海量存储设备、PC 硬盘和 ISO 镜像文件（磁盘镜像文件）。

注意：ISO9660 是 Raritan 支持的标准，但也可以使用其他 ISO 标准。

虚拟媒体允许你远程执行其他任务，例如：

- 传输文件
- 运行诊断
- 安装或修补应用程序
- 操作系统完整安装

这种扩展的 KVM 控制消除了对数据中心的大部分访问，节省时间和金钱，因此虚拟媒体显得非常有用。



图示符号			
1	桌面 PC	A	CD/DVD 驱动器
2	Dominion KX II	B	USB 海量存储设备
3	CIM	C	PC 硬盘
4	目标服务器	D	远程文件服务器（ISO 镜像文件）

使用虚拟媒体的前提

可以利用虚拟媒体功能安装最多两个（不同类型的）驱动器，这些驱动器必须是当前应用于目标服务器的 USB 配置文件所支持的驱动器。这些驱动器可以在 KVM 会话持续期间访问。

例如可以安装并使用一个特定的 CD-ROM，在会话结束时断开它。不过，CD-ROM 虚拟媒体"通道"将保持打开状态，以便你虚拟安装另一个 CD-ROM。只要 USB 配置文件支持 KVM 会话，在 KVM 会话关闭之前，这些虚拟媒体通道仍然保持打开状态。

在你希望从目标服务器连接的客户机或网络文件服务器上连接/加装相关介质，即可使用虚拟媒体。这不是前提，但在尝试访问此介质之前，必须这样做。

为了使用虚拟媒体，必须满足下列条件：

Dominion 设备

- 对于需要访问虚拟媒体的用户，必须设置设备权限允许访问相关端口，同时还必须设置这些端口的虚拟媒体访问权限（VM 访问端口权限）。在组一级设置端口权限。
- 设备和目标服务器之间必须有 USB 连接。
- 如果要使用 PC 共享，还必须在 Security Settings（安全设置）页上启用安全设置。**可选**
- 必须给要连接的 KVM 目标服务器选择正确的 USB 配置文件。

客户机 PC

- 某些虚拟媒体选项要求客户机 PC 有管理权限（例如整个设备的驱动器重定向）。

注意：如果使用 Microsoft Vista 或 Windows 7，禁用 User Account Control（用户帐号控制），或者选择 Run as Administrator when starting Internet Explorer（在启动 Internet Explorer 时作为管理员运行）。为此，单击 Start（开始）菜单，找到 IE，用右键单击它，选择 Run as Administrator（作为管理员运行）。

目标服务器

- KVM 目标服务器必须支持 USB 连接设备。
- 运行 Windows 2000 的 KVM 目标服务器必须安装了所有最新补丁。
- USB 2.0 端口速度较快，首选使用此类端口。



在 Windows 环境下通过 VKC 和 AKC 使用虚拟媒体

Windows XP® 操作系统管理员权限和标准用户权限不同于 Windows Vista® 操作系统和 Windows 7® 操作系统的管理员权限和标准用户权限。

如果在 Vista 或 Windows 7 上启用用户访问控制 (UAC)，它给用户提供访问应用程序所需的最低权限。例如针对 Internet Explorer® 增加的 Run as Administrator（作为管理员运行）选项允许用户执行管理员级任务，否则即使用户使用管理员登录名，也不能访问这些任务。

这两个功能都影响用户可通过 Virtual KVM Client (VKC) 和 Active KVM Client (AKC) 访问的虚拟媒体的类型。参看 Microsoft® 帮助文件，进一步了解这些功能及其用法。

下面列出在 Windows 环境下，用户可通过 VKC 和 AKC 访问的虚拟媒体类型。这些功能按客户机功能和虚拟媒体功能细分，每个 Windows 用户角色可以访问不同的功能。

Windows XP

- 如果在 Windows XP 环境下运行 VKC 和 AKC，用户必须具备管理员权限，才能访问除 CD-ROM 连接、ISO 和 ISO 镜像文件之外的任何虚拟媒体。

Windows Vista 和 Windows 7

- 如果在 Windows Vista 或 Windows 7 环境下运行 VKC 和 AKC，并且启用用户访问控制 (UAC)，可以访问下列虚拟媒体类型，视用户的 Windows 角色而定：

客户机	管理员	标准用户
AKC 和 VKC	访问： • 固定驱动器和固定驱动器分区 • 可拆卸驱动器 • CD/DVD 驱动器 • ISO 镜像文件 • 远程 ISO 镜像文件	访问： • 可拆卸驱动器 • CD/DVD 驱动器 • ISO 镜像文件 • 远程 ISO 镜像文件



使用虚拟媒体

参看使用虚拟媒体的前提，了解如何使用虚拟媒体。

► 使用虚拟媒体：

1. 如果要访问文件服务器 ISO 镜像文件，在 Remote Console File Server Setup（文件服务器设置）页上指定这些文件服务器和镜像文件。参看文件服务器设置（仅文件服务器 ISO 镜像文件）。

   注意：ISO9660 格式是 Raritan 支持的标准，但也可以使用其他 CD-ROM 扩展。

2. 与适当的目标服务器建立 KVM 会话。
   a. 在 Remote Console 上打开 Port Access（端口访问）页。
   b. 在 Port Access（端口访问）页上连接目标服务器：
   - 单击适当目标服务器的 Port Name（端口名称）。
   - 在 Port Action（端口操作）菜单上选择 Connect（连接）命令。在 Virtual KVM Client 窗口上打开目标服务器。

3. 连接虚拟媒体：

对于：	选择此虚拟媒体选项：
本地驱动器	本地驱动器
本地 CD/DVD 驱动器	CD-ROM/DVD-ROM/ISO 镜像文件
ISO 镜像文件	Connect CD-ROM/ISO Image（连接 CD-ROM/ISO 镜像文件）
文件服务器 ISO 镜像文件	Connect CD-ROM/ISO Image（连接 CD-ROM/ISO 镜像文件）

在完成任务之后，断开虚拟媒体。参看***断开虚拟媒体*** (p. 97)。



文件服务器设置（仅文件服务器 **ISO** 镜像文件）

注意：只有在用虚拟媒体访问文件服务器 ISO 镜像文件时，才需要此功能。

ISO9660 格式是 Raritan 支持的标准，但也可以使用其他 CD-ROM 扩展。

用 Remote Console File Server Setup（文件服务器设置）页指定要用虚拟媒体访问的文件服务器和镜像文件路径。在此指定的文件服务器 ISO 镜像文件，可以在 Map Virtual Media CD/ISO Image（映射虚拟媒体 CD/ISO 镜像文件）对话框上的 Remote Server ISO Image Hostname（远程服务器 ISO 镜像文件主机名）和 Image（镜像文件）下拉列表上选择。参看 **CD-ROM/DVD-ROM/ISO 镜像文件** (p. 95)。

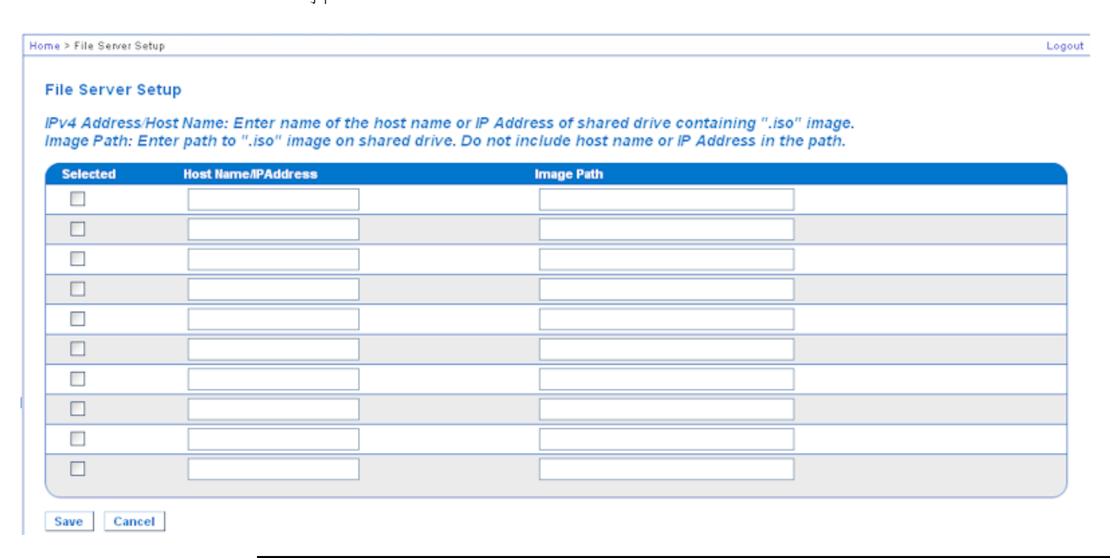
▶ **指定要通过虚拟媒体访问的文件服务器 ISO 镜像文件：**

1. 在 Remote Console 上选择 Virtual Media（虚拟媒体）。打开 File Server Setup（文件服务器设置）页。
2. 选择要作为虚拟媒体访问的所有介质对应的 Selected（选择）复选框。
3. 输入要访问的文件服务器 ISO 镜像文件的信息：
   - IP Address/Host Name（IP 地址/主机名）— 文件服务器的主机名或 IP 地址
   - Image Path（镜像文件路径）— ISO 镜像文件所在位置的全路径名

注意：主机名长度不能超过 232 个字符。



4. 单击 Save（保存）按钮。在此指定的所有介质，可以在 Map Virtual Media CD/ISO Image（映射虚拟媒体 CD/ISO 镜像文件）对话框上选择。



注意：由于 KX2 使用的第三方软件的技术限制，不能使用 IPv6 地址通过虚拟媒体访问远程 ISO 镜像文件。

注意：如果连接 Windows 2003 Server 并尝试加载服务器上的 ISO 镜像文件，系统显示错误消息："在端口安装虚拟媒体失败。不能连接文件服务器，或者文件服务器名称和密码错误。"如果发生这种情况，在服务器的 Domain Controllers（域控制器）策略下禁用 Microsoft Network Server: Digitally Sign Communications（Microsoft 网络服务器：数字签名通信）选项。



连接虚拟媒体

本地驱动器

此选项安装整个驱动器，这意味着采用虚拟方式将整个磁盘驱动器安装在目标服务器上。将此选项仅用于硬盘和外置驱动器。不包括网络驱动器、CD-ROM 驱动器或 DVD-ROM 驱动器。这是唯一一个有读写权限的选项。

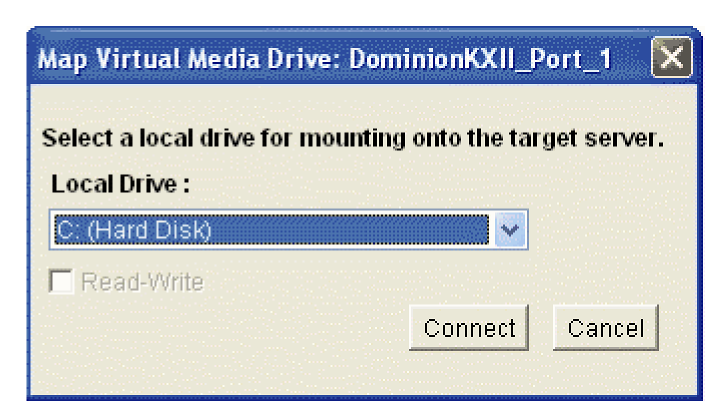
注意：运行某些版本的 Windows 操作系统的 KVM 目标服务器，在将一个 NTFS 格式化分区重定向到它们之后（例如 C 盘），它们可能不接受新的海量存储设备连接。

如果出现这些情况，关闭 Remote Console，重定向到另一个虚拟媒体设备，然后重新连接它。如果其他用户连接同一台目标服务器，他们也必须关闭目标服务器连接。

注意：对于 Dominion KX II 2.1.0 和更高版本，如果安装软驱等外置驱动器，驱动器上的 LED 指示灯常亮，因为设备每 500 毫秒检查一次驱动器，确认驱动器是否还在。

▶ 访问客户计算机上的驱动器：

1. 在 Virtual KVM Client 上选择 Virtual Media（虚拟媒体）> Connect Drive（连接驱动器）。打开 Map Virtual Media Drive（映射虚拟媒体驱动器）对话框。



2. 在 Local Drive（本地驱动器）下拉列表上选择驱动器。
3. 如果需要读写功能，选择 Read-Write（读写）复选框。不能拆卸的驱动器禁用此选项。参看***读写不可用时的条件*** (p. 95)了解详情。如果选择此复选框，可以读写连接的 USB 磁盘。

警告：启用读写访问可能很危险！从多个实体上同时访问同一个驱动器，可能会导致数据损坏。如果不需要写访问权，不要选择此复选框。



4. 单击 Connect（连接）。采用虚拟方式将此介质安装在目标服务器上。可以像访问其他驱动器一样访问此介质。

读写不可用时的条件

在下列情况下，虚拟媒体读写功能不可用：

- 对于所有硬盘。
- 当驱动器有写保护时。
- 当用户没有读写权限时：
  - Port Permission Access（端口权限访问）设置为 None（无）或 View（查看）。
  - Port Permission VM Access（端口权限虚拟媒体访问）设置为 Read-Only（只读）或 Deny（拒绝）。

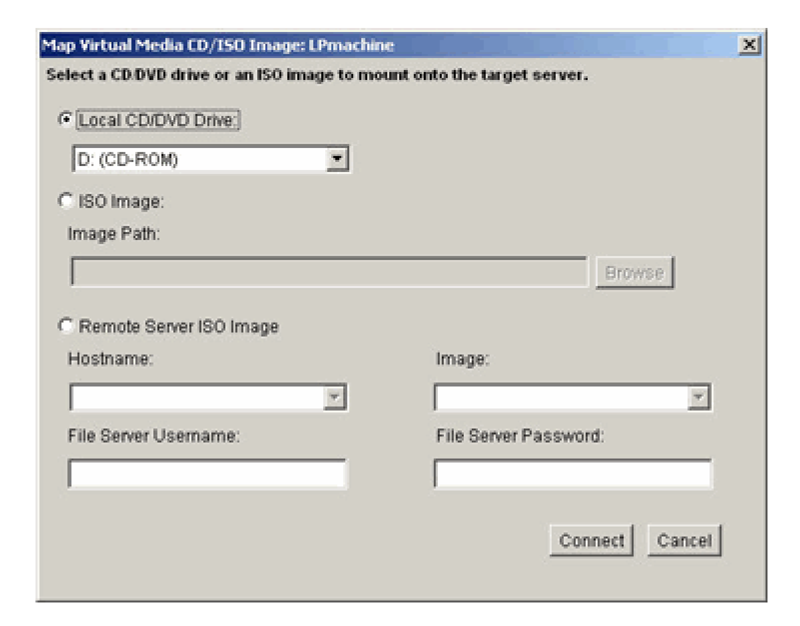
CD-ROM/DVD-ROM/ISO 镜像文件

此选项安装 CD-ROM、DVD-ROM 和 ISO 镜像文件。

注意：ISO9660 格式是 Raritan 支持的标准，但也可以使用其他 CD-ROM 扩展。

▶ 访问 CD-ROM、DVD-ROM 和 ISO 镜像文件：

1. 在 Virtual KVM Client 上选择 Virtual Media（虚拟媒体）> Connect CD-ROM/ISO Image（连接 CD-ROM/ISO 镜像文件）。打开 Map Virtual Media CD/ISO Image（映射虚拟媒体 CD/ISO 镜像文件）对话框。





2. 对于内置和外置 CD-ROM 驱动器或 DVD-ROM 驱动器：
    a. 选择 Local CD/DVD Drive（本地 CD/DVD 驱动器）选项。
    b. 在 Local CD/DVD Drive（本地 CD/DVD 驱动器）下拉列表上选择驱动器。下拉列表显示所有可用的内置和外置 CD 驱动器和 DVD 驱动器的名称。
    c. 单击 Connect（连接）。
3. 对于 ISO 镜像文件：
    a. 选择 ISO Image（ISO 镜像文件）选项。如果要访问 CD、DVD 或硬盘的磁盘镜像文件，使用此选项。ISO 格式是支持的唯一格式。
    b. 单击 Browse（浏览）按钮。
    c. 导航到要使用的磁盘镜像文件所在的路径，单击 Open（打开）。Image Path（镜像文件路径）字段自动填充该路径。
    d. 单击 Connect（连接）。
4. 对于文件服务器上的远程 ISO 镜像文件：
    a. 选择 Remote Server ISO Image（远程服务器 ISO 镜像文件）选项。
    b. 在 Hostname（主机名）和 Image（镜像文件）下拉列表上选择主机名和镜像文件。可以使用的文件服务器和镜像文件路径是你在 File Server Setup（文件服务器设置）页上配置的那些文件服务器和镜像文件路径。下拉列表只显示在 File Server Setup（文件服务器设置）页上配置的项目。
    c. File Server Username（文件服务器用户名）— 访问文件服务器所需的用户名。
    d. File Server Password（文件服务器密码）— 访问文件服务器所需的密码（输入时字段显示星号）。
    e. 单击 Connect（连接）。

采用虚拟方式将此介质安装在目标服务器上。可以像访问其他驱动器一样访问此介质。



注意：如果使用 Linux 目标系统上的文件，在虚拟媒体复制文件之后，用 Linux Sync（同步）命令查看复制的文件。在执行同步之前，可能不显示复制的文件。

注意：如果使用 Windows 7，在安装本地 CD/DVD 驱动器或本地/远程 ISO 镜像文件时，Window 的 My Computer（我的计算机）文件夹默认不显示 Removable Disk（可拆卸磁盘）。如要在此文件夹里查看本地 CD/DVD 驱动器或本地/远程 ISO 镜像文件，选择 Tools（工具）> Folder Options（文件夹选项）>视图，取消 Hide empty drives in the Computer folder（计算机文件夹隐藏空驱动器）。

注意：由于 KX2 使用的第三方软件的技术限制，不能使用 IPv6 地址通过虚拟媒体访问远程 ISO 镜像文件。

断开虚拟媒体

▶ 断开虚拟媒体驱动器：

- 对于本地驱动器，选择 Virtual Media（虚拟媒体）> Disconnect Drive（断开驱动器）。
- 对于 CD-ROM、DVD-ROM 和 ISO 镜像文件，选择 Virtual Media（虚拟媒体）> Disconnect CD-ROM/ISO Image（断开 CD-ROM/ISO 镜像文件）。

注意：除了用 Disconnect（断开）命令断开虚拟媒体，关闭 KVM 连接也同时关闭虚拟媒体。

Ch 6 USB 配置文件

在本章内

概述

为了使 Dominion KX II 能支持更多不同的 KVM 目标服务器，Raritan 针对众多操作系统级和 BIOS 级服务器实现推出一组标准的 USB 配置文件。

Generic（默认值）USB 配置文件可满足部署的绝大多数 KVM 目标服务器配置的要求。还提供其他配置文件满足其他常部署的服务器配置（例如 Linux® 和 Mac OS X®）的特定要求。还有许多配置文件（用平台名称和 BIOS 版本号命名）可增强目标服务器的虚拟媒体功能，例如在 BIOS 级操作时。

USB 配置文件在 Dominion KX II Remote Console 和 Dominion KX II Local Console 的 Device Settings（设备设置）> Port Configuration（端口配置）> Port（端口）页上配置。设备管理员可以给端口配置最能满足用户需求和目标服务器配置需求的配置文件。

连接 KVM 目标服务器的用户可以根据 KVM 目标服务器的工作状态，在 ***Virtual KVM Client*** (p. 52) 上选择这些预先选择的配置文件。例如假如服务器正在运行，用户想使用 Windows® 操作系统，最好使用 Generic 配置文件。但如果用户要在 BIOS 菜单上更改设置，或者要用虚拟媒体启动，BIOS 配置文件可能更合适，视目标服务器型号而定。

如果给定的 KVM 目标服务器不能使用 Raritan 提供的任何一个标准 USB 配置文件，请联系 Raritan 技术支持部门寻求协助。



CIM 兼容性

为了使用 USB 配置文件，必须使用安装了最新固件的 D2CIM-VUSB 或 D2CIM-DVUSB。尚未升级固件的 VM-CIM 支持许多配置（键盘、鼠标、CD-ROM 和可拆卸驱动器），但不能使用那些针对特定目标服务器配置优化过的配置文件。除此之外，为了访问 USB 配置文件，还应该将现有 VM-CIM 的固件升级到最新版本。在升级现有 VM-CIM 之前，它们具备的功能相当于 Generic 配置文件的功能。

在 Dominion KX II 固件升级过程中自动升级 VM-CIM 固件，但可以如***升级 CIM*** (p. 210) 所述对那些尚未升级固件的 VM-CIM 进行升级。

参看***计算机接口模块 (CIM)*** (p. 254) 了解其他信息。

可用的 USB 配置文件

最新版 Dominion KX II 配备如下表所述的 USB 配置文件。Raritan 提供的每次固件升级均包括新配置文件。在增加新配置文件时，在帮助中加以说明。

USB 配置文件	说明
BIOS Dell® PowerEdge® 1950/2950/2970/6950/R200	Dell PowerEdge 1950/2950/2970/6950/R200 BIOS 将此配置文件或 Generic 配置文件用于 Dell PowerEdge 1950/2950/2970/6950/R200 BIOS。 限制： • 无
仅 BIOS DellOptiplex 键盘	Dell Optiplex BIOS 访问（仅键盘） 在使用 D2CIM-VUSB 时，用此配置文件给 Dell Optiplex BIOS 提供键盘功能。在使用新的 D2CIM-DVUSB 时，使用 Generic 配置文件。 注意： • Optiplex 210L/280/745/GX620 需要 D2CIM-DVUSB 和 Generic 配置文件才能支持虚拟媒体 限制： • USB 总线速度限于全速 (12 MBps) • 不支持虚拟媒体



<table>
<tr><th>USB 配置文件</th><th>说明</th></tr>
<tr><td>仅 BIOS DellPowerEdge 键盘</td><td>Dell PowerEdge BIOS 访问（仅键盘）

在使用 D2CIM-VUSB 时，用此配置文件给 Dell PowerEdge BIOS 提供键盘功能。在使用新的 D2CIM-DVUSB 时，使用 Generic 配置文件。

注意：
• PowerEdge 650/1650/1750/2600/2650 BIOS 不支持 USB CD-ROM 和磁盘驱动器作为启动盘
• PowerEdge 750/850/860/1850/2850/SC1425 BIOS 需要 D2CIM-DVUSB 和 Generic 配置文件才能支持虚拟媒体
• 在 BIOS 下操作时，将 BIOS Dell PowerEdge 1950/2950/2970/6950/R200 或 Generic 配置文件用于 PowerEdge 1950/2950/2970/6950/R200

限制：
• USB 总线速度限于全速 (12 MBps)
• 不支持绝对鼠标同步™
• 不支持虚拟媒体</td></tr>
<tr><td>BIOS Generic</td><td>BIOS Generic

当 Generic 操作系统配置文件对 BIOS 不起作用时，使用此配置文件。

警告：每当连接或断开虚拟媒体时，均触发 USB 枚举。

限制：
• USB 总线速度限于全速 (12 MBps)
• 不支持绝对鼠标同步™
• 不能同时使用虚拟 CD-ROM 和磁盘驱动器</td></tr>
<tr><td>BIOS HP® Proliant™ DL145</td><td>HP Proliant DL145 PhoenixBIOS

在操作系统安装过程中，将此配置文件用于 HP Proliant DL145 PhoenixBIOS。</td></tr>
</table>



USB 配置文件	说明
	限制： • USB 总线速度限于全速 (12 MBps)
BIOS HP Compaq® DC7100/DC7600	BIOS HP Compaq DC7100/DC7600 使用此配置文件，用虚拟媒体启动 HP Compaq DC7100/DC7600 系列台式机。 限制： • 不能同时使用虚拟 CD-ROM 和磁盘驱动器
BIOS IBM ThinkCentre Lenovo	IBM Thinkcentre Lenovo BIOS 在 BIOS 操作过程中，将此配置文件用于 IBM® Thinkcentre Lenovo 系统板（828841U 型）。 限制： • USB 总线速度限于全速 (12 MBps) • 不能同时使用虚拟 CD-ROM 和磁盘驱动器
BIOS Lenovo ThinkPad T61 和 X61	BIOS Lenovo ThinkPad T61 和 X61（用虚拟媒体启动） 使用此配置文件，用虚拟媒体启动 T61 和 X61 系列笔记本。 限制： • USB 总线速度限于全速 (12 MBps)
BIOS Mac	BIOS Mac 将此配置文件用于 Mac® BIOS。 限制： • 不支持绝对鼠标同步™ • 不能同时使用虚拟 CD-ROM 和磁盘驱动器
Generic	Generic USB 配置文件的特性类似旧版 KX2 的特性。将此配置文件用于 Windows 2000® 操作系统、Windows XP® 操作系统、Windows Vista® 操作系统和更高版本。 限制： • 无

USB 配置文件	说明
HP Proliant DL360/DL380 G4 (HP SmartStart CD)	HP Proliant DL360/DL380 G4 (HP SmartStart CD) 在用 HP SmartStart CD 安装操作系统时，将此配置文件用于 HP Proliant DL360/DL380 G4 系列服务器。 限制： • USB 总线速度限于全速 (12 MBps) • 不支持绝对鼠标同步™
HP Proliant DL360/DL380 G4 (Windows 2003® Server Installation)	HP Proliant DL360/DL380 G4（Windows 2003 Server 安装） 在不用 HP SmartStart CD 安装 Windows 2003 Server 时，将此配置文件用于 HP Proliant DL360/DL380 G4 系列服务器。 限制： • USB 总线速度限于全速 (12 MBps)
Linux®	通用 Linux 配置文件 这是通用 Linux 配置文件；将它用于 Redhat Enterprise Linux、SuSE Linux Enterprise Desktop 和其他分发版本。 限制： • 不支持绝对鼠标同步™
MAC OS X®（10.4.9 和更高版本）	MAC OS-X v10.4.9 和更高版本 此配置文件补偿最新版 Mac OS-X 引入的鼠标坐标缩放比例。如果远程鼠标位置和本地鼠标位置在桌面边沿附近不同步，就选择此选项。 限制： • 不能同时使用虚拟 CD-ROM 和磁盘驱动器
RUBY Industrial Mainboard (AwardBIOS)	RUBY Industrial Mainboard (AwardBIOS) 将此配置文件用于采用 Phoenix/AwardBIOS v6.00PG 的 RUBY-9715VG2A 系列工业主板。 限制：



<table>
<tr><th>USB 配置文件</th><th>说明</th></tr>
<tr><td></td><td>USB 总线速度限于全速 (12 MBps)
不能同时使用虚拟 CD-ROM 和磁盘驱动器</td></tr>
<tr><td>Supermicro Mainboard Phoenix (AwardBIOS)</td><td>Supermicro Mainboard Phoenix AwardBIOS
将此配置文件用于采用 Phoenix/AwardBIOS 的 Supermicro 系列主板。
限制：
不能同时使用虚拟 CD-ROM 和磁盘驱动器</td></tr>
<tr><td>Suse 9.2</td><td>SuSE Linux 9.2
将此配置文件用于 SuSE Linux 9.2 分发版本。
限制：
不支持绝对鼠标同步™
USB 总线速度限于全速 (12 MBps)</td></tr>
<tr><td>Troubleshooting 1</td><td>Troubleshooting 配置文件 1
第一海量存储设备
键盘和鼠标 (Type 1)
USB 总线速度限于全速 (12 MBps)
不能同时使用虚拟 CD-ROM 和磁盘驱动器
警告：每当连接或断开虚拟媒体时，均触发 USB 枚举。</td></tr>
<tr><td>Troubleshooting 2</td><td>Troubleshooting 配置文件 2
第一键盘和鼠标 (Type 2)
海量存储设备
USB 总线速度限于全速 (12 MBps)
不能同时使用虚拟 CD-ROM 和磁盘驱动器
警告：每当连接或断开虚拟媒体时，均触</td></tr>
</table>



USB 配置文件	说明
	发 USB 枚举。
Troubleshooting 3	Troubleshooting 配置文件 3 • 第一海量存储设备 • 键盘和鼠标 (Type 2) • USB 总线速度限于全速 (12 MBps) • 不能同时使用虚拟 CD-ROM 和磁盘驱动器 警告：每当连接或断开虚拟媒体时，均触发 USB 枚举。
Use Full Speed for Virtual Media CIM	虚拟媒体 CIM 使用全速 此配置文件的特性类似旧版 KX2 在选择 Full Speed for Virtual Media CIM（虚拟媒体 CIM 全速）选项时的特性。可用于那些不能处理高速 USB 设备的 BIOS。 限制： • USB 总线速度限于全速 (12 MBps)

给 KVM 端口选择配置文件

Dominion KX II 配备一组 USB 配置文件，你可以根据 KVM 端口所连的 KVM 目标服务器的特性，给 KVM 端口指定这些配置文件。可以在 Device Settings（设备设置）> Port Configuration（端口配置）> Port（端口）页、Dominion KX II Remote Console 或 Dominion KX II Local Console 上给 KVM 端口指定 USB 配置文件。

指定配置文件的管理员很可能必须是特定目标服务器的管理员。在此之后，可以通过 MPC/VKC 选择这些配置文件。如果尚未指定配置文件，可以选择 USB Profile（USB 配置文件）> Other Profiles（其他配置文件）访问任何一个可用的配置文件。

在给 KVM 端口指定 USB 配置文件之后，当用户连接 KVM 目标服务器时，可以使用这些配置文件。如有必要，用户可以在 VKC 或 VPC 的 USB Profile（USB 配置文件）菜单上选择一个 USB 配置文件。

参看***配置 USB 配置文件（端口页）*** (p. 182)，了解如何给 KVM 端口指定 USB 配置文件。



在与 DCIM-VUSB 一起使用 Mac OS-X USB 配置文件时的鼠标模式

如果使用 DCIM-VUSB 和 Max OS-X® USB 配置文件，并运行 Mac OS-X 10.4.9（或更高版本），必须在单鼠标模式下重新启动，才能在 Boot（启动）菜单上使用鼠标。

▶ **配置要在启动菜单上使用的鼠标：**

1. 重新启动 Mac，在重新启动过程中按 Option 键打开 Boot（启动）菜单。此时鼠标没有响应。
2. 选择 Intelligent Mouse（智能鼠标）模式，然后 Single Mouse（单鼠标）模式。鼠标响应。

   注意：在 Single Mouse（单鼠标）模式下，鼠标速度可能很慢。

3. 在退出 Boot（启动）菜单启动操作系统之后，退出 Single Mouse（单鼠标）模式，切换回 Absolute Mouse（绝对鼠标）模式提高鼠标性能。



Ch 7 用户管理

在本章内

用户组

Dominion KX II 在内部存储所有用户名和组名的列表，以便确定访问权和权限。这些信息在内部采用加密格式存储。有几种验证方式，这种验证方式称为本地验证。必须验证所有用户。如果给 Dominion KX II 配置了 LDAP/LDAPS 或 RADIUS，先进行此验证，再进行本地验证。

每台 Dominion KX II 有三个默认用户组。不能删除这些用户组：

User（用户）	说明
Admin（管理员）	本组用户具有所有管理权限。出厂前默认的最初用户是本组的成员，具有所有系统权限。此外，Admin 用户必须是 Admin 组的成员。
Unknown（未知）	这是那些用 LDAP/LDAPS 或 RADIUS 进行外部验证或系统未知的用户的默认组。如果外部 LDAP/LDAPS 或 RADIUS 服务器不确定一个有效用户组，就使用 Unknown（未知）组。此外，新创建的任何用户均自动放入此组，直到给他们指定另一个组为止。
Individual Group（个人组）	个人组基本上是一个人的“组”。也就是说，特定用户位于自己的组里，与其他实际组没有关联。可以在组名称里使用 @ 符号，表示这是个人组。个人组允许一个用户帐号具有与一个组相同的权限。

在 Dominion KX II 上最多可以创建 254 个用户组。

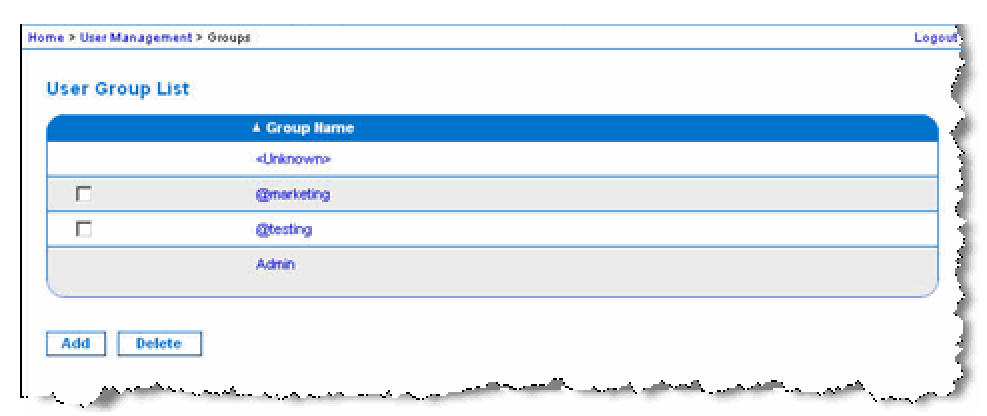
用户组列表

在本地验证和远程验证（通过 RADIUS 或 LDAP/LDAPS 进行的）中，要使用用户组。在创建个人用户之前定义用户组是个好主意，因为在添加一个用户时，必须给该用户指定一个现有用户组。

User Group List(用户组列表)页显示所有用户组的列表，可以单击 Group Name（组名称）列标题，按升序顺序或降序顺序排序用户组。还可以在 User Group List（用户组列表）页上添加、修改或删除用户组。

▶ 列出用户组：

- 选择 User Management（用户管理）> User Group List（用户组列表）。打开 User Group List（用户组列表）页。



用户和组之间的关系

用户属于一个组，组有权限。将 Dominion KX II 的众多用户分成组，同时管理一个组里所有用户的权限，而不是分别管理每个用户的权限，这样可以节省时间。

也可以选择不让特定用户与组关联。在此情况下，可以将此用户归入 Individual（个人）。

在成功验证之后，设备用用户组信息确定用户权限，例如哪些服务器端口可以访问，是否允许重新启动设备，能否执行其他功能。

添加新用户组

▶ 添加新用户组：

1. 选择 User Management（用户管理）> Add New User Group（添加新用户组），或者单击 User Group List（用户组列表）页上的 Add（添加）按钮，打开 Group（用户组）页。

Group（用户组）页按下列类别组织管理：Group（组）、Permissions（权限）、Port Permissions（端口权限）和 IP ACL（IP 访问控制表）。

2. 在 Group Name（组名）字段里输入新用户组的说明性名称（最多 64 个字符）。
3. 给该组设置 Permissions（权限）。选择要给此组所有用户指定的权限前面的复选框。 参看***设置权限*** (p. 110)。
4. 设置 Port Permissions（端口权限）。指定此组的用户可以访问的服务器端口（和访问类型）。 参看***设置端口权限*** (p. 111)。
5. 设置 IP ACL（IP 访问控制表）。此功能通过指定 IP 地址来限制对 Dominion KX II 设备的访问。此功能仅应用于属于特定组的用户，与 IP 访问控制表功能不一样，后者应用于对设备进行的所有访问（并确定优先级）。 **可选**。参看***基于组的 IP 访问控制表*** (p. 112)。
6. 单击 OK（确定）按钮。



注意：在 MPC 和 Dominion KX II Local Console 上可以使用几个管理功能。这些功能只能供默认 Admin（管理员）组的成员使用。

注意：同时支持 IPv4 地址和 IPv6 地址。

Home > User Management > Group

Group

Group Name *

▼ Permissions

- ☑ Device Access While Under CC-SG Management
- ☑ Device Settings
- ☑ Diagnostics
- ☑ Maintenance
- ☑ Modem Access
- ☑ PC-Share
- ☑ Security
- ☑ User Management

▼ Port Permissions

Port	Access	VM Access	Power Control
1: BC_Port1_R8_from_KX	Deny	Deny	Deny
1-1: BC_Port1_Slot1_To_Local_Port	Deny	Deny	Deny
1-2: Blade_Chassis_Port1_Slot2	Deny	Deny	Deny
1-3: Blade_Chassis_Port1_Slot3	Deny	Deny	Deny
1-4: Blade_Chassis_Port1_Slot4	Deny	Deny	Deny
1-5: Blade_Chassis_Port1_Slot5	Deny	Deny	Deny
1-6: Blade_Chassis_Port1_Slot6	Deny	Deny	Deny
1-7: Blade_Chassis_Port1_Slot7	Deny	Deny	Deny
1-8: Blade_Chassis_Port1_Slot8	Deny	Deny	Deny
1-9: Blade_Chassis_Port1_Slot9	Deny	Deny	Deny
1-10: Blade_Chassis_Port1_Slot10	Deny	Deny	Deny
1-11: Blade_Chassis_Port1_Slot11	Deny	Deny	Deny
1-12: Blade_Chassis_Port1_Slot12	Deny	Deny	Deny
1-13: Blade_Chassis_Port1_Slot13	Deny	Deny	Deny
1-14: Blade_Chassis_Port1_Slot14	Deny	Deny	Deny
1-15: Blade_Chassis_Port1_Slot15	Deny	Deny	Deny
1-16: Blade_Chassis_Port1_Slot16	Deny	Deny	Deny
2: KX2_Port2_R9_from_CC	Deny	Deny	Deny
3: KX2_Port2_R9_from_CC	Deny	Deny	Deny
	☐ Set All to Deny	☐ Set All VM Access to Deny	☐ Set All Power to Deny
	☐ Set All to View	☐ Set All VM Access to Read-Only	
	☐ Set All to Control	☐ Set All VM Access to Read-Write	☐ Set All Power to Access

▼ IP ACL

Rule #	Starting IP	Ending IP	Action
			ACCEPT

Append | Insert | Replace | Delete

OK | Cancel



设置权限

重要说明：如果选择 User Management（用户管理）复选框，允许组成员更改所有用户的权限，包括自己的权限。认真考虑是否要授予这些权限。

权限	说明
Device Access While Under CC-SG Management（在 CC-SG 管理下进行设备访问）	在 CC-SG 上针对 Dominion KX II 设备启用 Local Access（本地访问）之后，允许有此权限的用户和用户组用 IP 地址直接访问此设备。可以在 Local Console、Remote Console、MPC、VKC 和 AKC 上访问此设备。 在直接访问受 CC-SG 管理的设备时，在 Dominion KX II 上记录访问和连接活动。根据 Dominion KX II 验证设置执行用户验证。 *注意：Admin（管理）用户组默认有此权限。*
Device Settings（设备设置）	网络设置、日期/时间设置、端口配置（通道名称和电源关联）、事件管理（SNMP 和系统日志）、虚拟媒体文件服务器设置。
Diagnostics（诊断）	网络接口状态、网络统计信息、ping 主机、跟踪到主机的路由、Dominion KX II 诊断。
Maintenance（维护）	备份和恢复数据库、固件升级、工厂复位、重新引导。
Modem Access（调制解调器访问）	用调制解调器连接 Dominion KX II 设备所需的权限。
PC-Share（PC 共享）	多个用户同时访问同一个目标。 如果使用级联配置，用基础 Dominion KX II 设备访问多台其他级联设备，单击基础设备名称左边的展开箭头图标 ，在 Port Access（端口访问）页上查看级联设备。 所有设备必须共享相同的 PC 共享设置。参看***配置和启用级联*** (p. 137)详细了解级联。
Security（安全）	SSL 证书、安全设置（VM 共享和 PC 共享）、IP ACL。
User Management（用户管理）	用户和组管理、远程验证 (LDAP/LDAPS/RADIUS)、登录设置。



权限	说明
	如果使用级联配置，用基础 Dominion KX II 设备访问多台其他级联设备，所有设备上的用户设置、用户组设置和远程验证设置必须保持一致。参看***配置和启用级联*** (p. 137)详细了解级联。

设置端口权限

对于每个服务器端口，可以指定用户组具有的访问类型，以及虚拟媒体和电源控制的端口访问类型。请注意所有权限的默认设置是 Deny（拒绝）。

端口访问	
选项	说明
Deny（拒绝）	彻底拒绝访问
View（查看）	查看视频，但不与相连的目标服务器交互操作
Control（控制）	控制相连的目标服务器。如果同时授予虚拟媒体访问权和电源控制访问权，必须给该组指定控制。

虚拟媒体访问	
选项	说明
Deny（拒绝）	端口彻底拒绝虚拟媒体权限
Read-Only（只读）	虚拟媒体访问仅限于读访问
Read-Write（读写）	虚拟媒体全访问（读写）



电源控制访问	
选项	**说明**
Deny（拒绝）	拒绝对目标服务器进行电源控制
Access（访问）	目标服务器电源控制全访问

对于刀片服务器机箱，端口访问权限将控制对给刀片服务器机箱配置的 URL 的访问权。选项是 Deny（拒绝）或 Control（控制）。此外，机箱上的每个刀片服务器都有自己的独立端口权限设置。

如果使用级联配置，用基础 Dominion KX II 设备访问多台其他级联设备，单击基础设备名称左边的展开箭头图标 ，在 Port Access（端口访问）页上查看级联设备。级联设备执行逐个端口控制。 参看*配置和启用级联* (p. 137)详细了解级联。

设置个人组权限

▶ 设置个人用户组权限：

1. 在列出的用户组中找到个人用户组。个人组的组名里可能使用 @ 符号。
2. 单击 Group Name（组名称）。打开 Group（用户组）页。
3. 选择适当的权限。
4. 单击 OK（确定）按钮。

注意：如果使用备用 RADIUS 验证，参看备用 RADIUS 验证设置进一步了解设置。

基于组的 IP 访问控制表

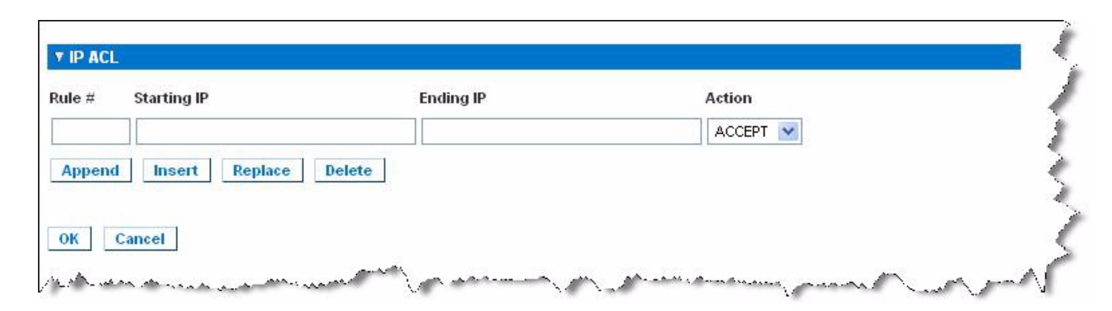
重要说明：在使用基于组的 IP 访问控制时务必谨慎。如果 IP 地址在拒绝访问的地址范围内，可能无法访问 Dominion KX II。

此功能按所选组里的用户，将 Dominion KX II 设备访问限于特定 IP 地址。此功能仅应用于属于特定组的用户，与 IP 访问控制表功能不一样，后者应用于对设备进行的所有访问，首先处理，并确定优先级。

重要说明：不能封锁 Dominion KX II 本地端口使用的 IP 地址 127.0.0.1。



使用 Group（用户组）页的 IP ACL 部分，根据用户组添加、插入、替换和删除 IP 访问控制规则。



▶ 添加（附加）规则：

1. 在 Starting IP（开始 IP）字段里输入开始 IP 地址。
2. 在 Ending IP（结束 IP）字段里输入结束 IP 地址。
3. 在可用选项中选择操作：
   - Accept（接受）— 设置为 Accept（接受）的 IP 地址允许访问 Dominion KX II 设备。
   - Drop（拒绝）— 设置为 Drop（拒绝）的 IP 地址拒绝访问 Dominion KX II 设备。
4. 单击 Append（附加）。此规则被添加到规则列表末尾。对于要输入的每个规则，重复第一步到第四步。

▶ 插入规则：

1. 输入规则编号 (#)。在使用 Insert（插入）命令时，需要规则编号。
2. 在 Starting IP（开始 IP）和 Ending IP（结束 IP）字段里分别输入开始 IP 地址和结束 IP 地址。
3. 在 Action（操作）下拉列表上选择操作。
4. 单击 Insert（插入）。如果输入的规则编号与现有规则编号相同，将新规则放在现有规则前面，列表上的所有规则向下移。

▶ 替换规则：

1. 指定要替换的规则编号。
2. 在 Starting IP（开始 IP）和 Ending IP（结束 IP）字段里分别输入开始 IP 地址和结束 IP 地址。
3. 在 Action（操作）下拉列表上选择操作。
4. 单击 Replace（替换）。新规则取代规则编号相同的旧规则。

▶ 删除规则：

1. 指定要删除的规则编号。
2. 单击 Delete（删除）按钮。
3. 在系统提示你确认删除时，单击 OK（确定）按钮。

重要说明：按 ACL 规则的输入顺序对它们求值。例如此处的示例，如果两个 ACL 规则的顺序相反，Dominion 根本不接受通信。

```
Rule 1, Starting IP = 192.168.50.1, Ending IP = 192.168.55.255, Action = ACCEPT

Rule 2, Starting IP = 0.0.0.0, Ending IP = 255.255.255.255, Action = DROP
```

提示：规则编号便于你更好地控制规则创建顺序。

注意：同时支持 IPv4 地址和 IPv6 地址。

修改现有用户组

注意：启用（但不能更改）Admin（管理员）组的所有权限。

▶ 修改现有用户组：

1. 在 Group（用户组）页上更改适当的字段，设置适当的权限。
2. 给该组设置 Permissions（权限）。选择要给此组所有用户指定的权限前面的复选框。参看设置权限。
3. 设置 Port Permissions（端口权限）。指定此组的用户可以访问的服务器端口（和访问类型）。参看**设置端口权限** (p. 111)。
4. 设置 IP ACL（IP 访问控制表）（可选）。此功能通过指定 IP 地址来限制对 Dominion KX II 设备的访问。参看**基于组的 IP 访问控制表** (p. 112)。
5. 单击 OK（确定）按钮。

▶ 删除用户组：

重要说明：如果删除有用户的组，自动给这些用户指定 <unknown>（未知）用户组。



提示：为了确定特定用户组的用户，按 User Group（用户组）排序 User List（用户列表）。

1. 单击 Group Name（组名称）左边的复选框，在列出的组中选择一个组。
2. 单击 Delete（删除）按钮。
3. 在系统提示你确认删除时，单击 OK（确定）按钮。

用户

必须给用户指定用户名和密码，才能访问 Dominion KX II。当用户尝试访问 Dominion KX II 时，要用这些信息验证用户。 最多可以给每个用户组创建 254 个用户。

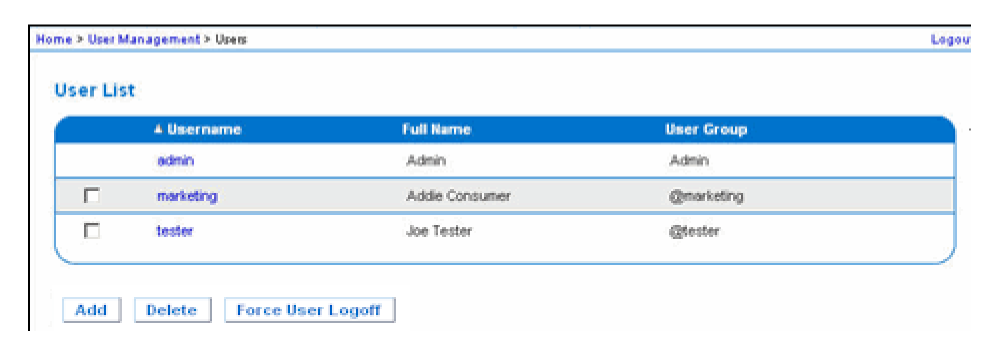
如果使用级联配置，用基础 Dominion KX II 设备访问多台其他级联设备，单击基础设备名称左边的展开箭头图标 ，在 Port Access（端口访问）页上查看级联设备。用户需要拥有访问基础设备所需的权限，以及在必要时访问各台级联设备所需的权限。当用户登录到基础设备时，查询每台级联设备，用户可以访问他们有权限的每台目标服务器。 参看***配置和启用级联*** (p. 137)详细了解级联。

用户列表

User List（用户列表）页显示所有用户的列表，包括他们的用户名、全名和用户组。可以单击任何一个列名称，按任何一列排序列表。还可以在 User List（用户列表）页上添加、修改或删除用户。

▶ 查看用户列表：

- 选择 User Management（用户管理）> User List（用户列表）。打开 User List（用户列表）页。





添加新用户

在创建 Dominion KX II 用户之前定义用户组是个好主意，因为在添加一个用户时，必须给该用户指定一个现有用户组。参看**添加新用户组** (p. 107)。

可以在 User（用户）页上添加新用户，修改用户信息，重新激活被停用的用户。

*注意：在登录失败次数超过在 Security Settings（安全设置）页上设置的最大登录尝试次数之后，可以停用用户名。参看**安全设置**。*

▶ 添加新用户：

1. 选择 User Management（用户管理）> Add New User（添加新用户），或者单击 User List（用户列表）页上的 Add（添加）按钮，打开 User（用户）页。
2. 在 Username（用户名）字段里输入唯一姓名（最长 16 个字符）。
3. 在 Full Name（全名）字段里输入用户全名（最长 64 个字符）。
4. 在 Password（密码）字段里输入密码，在 Confirm Password（确认密码）字段里再次输入密码（最长 64 个字符）。
5. 在 User Group（用户组）下拉列表上选择用户组。除了系统提供的默认组，此列表还包含你创建的所有组。<Unknown>（未知，默认设置）、Admin（管理员）、Individual Group（个人组）。

   如果不想使此用户与现有 User Group（用户组）关联，在下拉列表上选择 Individual Group（个人组）。如要进一步了解如何设置个人组权限，参看***设置个人组权限*** (p. 112)。
6. 如要激活此新用户，选择 Active（活动）复选框。默认值是 activated（激活，启用）。
7. 单击 OK（确定）按钮。

修改现有用户

▶ 修改现有用户：

1. 选择 User Management（用户管理）> User List（用户列表），打开 User List（用户列表）页。
2. 在 User List（用户列表）页列出的用户中找到要修改的用户。
3. 单击用户名。打开 User（用户）页。
4. 在 User（用户）页上更改适当的字段。参看***添加新用户*** (p. 116)，了解如何访问 User（用户）页。



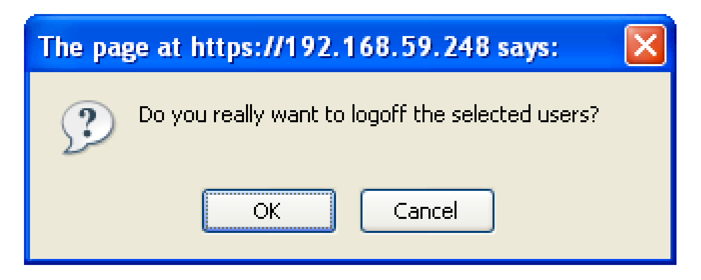
5. 如要删除用户，单击 Delete（删除）按钮。系统提示你确认删除。
6. 单击 OK（确定）按钮。

退出用户（强制退出）

如果你是管理员，可以让另一个在本地验证、已登录 Dominion KX II 的用户退出来。

退出用户：

1. 选择 User Management（用户管理）> User List（用户列表），或者单击页面左面板上的 Connected User（已连接用户）链接，打开 User List（用户列表）页。
2. 在 User List（用户列表）页列出的用户中找到要退出的用户，选择他们的姓名旁边的复选框。
3. 单击 Force User Logoff（强制用户退出）按钮。
4. 单击 Logoff User（退出用户）对话框上的 OK（确定）按钮，强制用户退出。



5. 显示一条确认消息，说明用户退出了。此消息包括退出日期和时间。单击 OK（确定）按钮关闭消息。



验证设置

验证是确定用户是否是他/她声称的人这一过程。在验证用户之后，用该用户的组确定其系统权限和端口权限。用户的指定权限决定授予他/她哪种访问权。这叫授权。

如果给 Dominion KX II 配置了远程验证，外部验证服务器主要用于验证，而不是授权。

如果使用级联配置，用基础 Dominion KX II 设备访问多台其他级联设备，单击基础设备名称左边的展开箭头图标 ，在 Port Access（端口访问）页上查看级联设备。基础设备和级联设备必须使用相同的验证设置。

可以在 Authentication Settings（验证设置）页上配置在访问 Dominion KX II 时所用的验证的类型。

注意：即使选择远程验证（LDAP/LDAPS 或 RADIUS），如果找不到用户，仍然选择本地验证数据库。

▶ **配置验证：**

1. 选择 User Management（用户管理）> Authentication Settings（验证设置）。打开 Authentication Settings（验证设置）页。
2. 选择要使用的验证协议选项（Local Authentication[本地验证]、LDAP/LDAPS 或 RADIUS）。如果选择 LDAP 选项，激活其余 LDAP 字段；如果选择 RADIUS 选项，激活其余 RADIUS 字段。
3. 如果选择 Local Authentication（本地验证），跳到第六步。
4. 如果选择 LDAP/LDAPS，阅读实现 LDAP 远程验证一节，了解如何填写 Authentication Settings（验证设置）页上 LDAP 部分的字段。
5. 如果选择 RADIUS，阅读实现 RADIUS 远程验证一节，了解如何填写 Authentication Settings（验证设置）页上 RADIUS 部分的字段。
6. 单击 OK（确定）按钮保存设置。

▶ **恢复出厂前默认设置：**

- 单击 **Reset to Defaults（复位到默认值）按钮。**



实现 LDAP/LDAPS 远程验证

Lightweight Directory Access Protocol (LDAP/LDAPS) 是联网协议，用于查询基于 TCP/IP 运行的目录服务。客户机连接 LDAP/LDAPS 服务器（默认 TCP 端口是 389），开始 LDAP 会话。客户机给服务器发送操作请求，服务器返回响应。

提示：Microsoft Active Directory 在本机充当 LDAP/LDAPS 验证服务器。

▶ 使用 LDAP 验证协议：

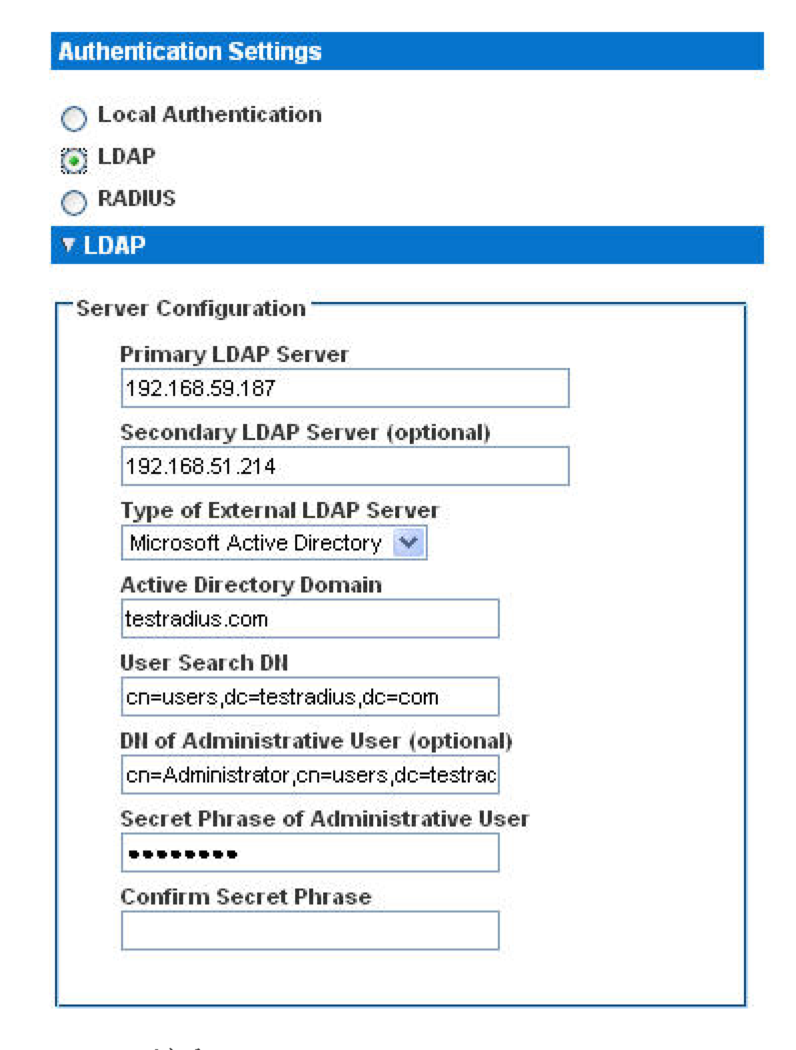
1. 单击 User Management（用户管理）> Authentication Settings（验证设置），打开 Authentication Settings（验证设置）页。
2. 选择 LDAP 单选按钮启用本页的 LDAP 部分。
3. 单击 ▸ LDAP 图标展开本页的 LDAP 部分。

服务器配置

4. 在 Primary LDAP Server（主 LDAP 服务器）字段里输入 LDAP/LDAPS 远程验证服务器的 IP 地址或 DNS 名称（最多 256 个字符）。在选择 Enable Secure LDAP（启用安全 LDAP）选项和 Enable LDAPS Server Certificate Validation（启用 LDAPS 服务器证书验证）选项之后，必须使用 DNS 名称与 LDAP 服务器证书的 CN 相匹配。
5. 在 Secondary LDAP Server（备用 LDAP 服务器）字段里输入 LDAP/LDAPS 服务器的 IP 地址或 DNS 名称（最多 256 个字符）。在选择 Enable Secure LDAP（启用安全 LDAP）选项之后，必须使用 DNS 名称。注意其他字段共享 Primary LDAP Server（主 LDAP 服务器）字段的设置。**可选**
6. 外部 LDAP 服务器的类型。
7. 输入 Active Directory Domain（Active Directory 域）的名称，例如 *testradius.com*。向 Active Directory 管理员索取特定域名。
8. 在 User Search DN（用户搜索标识名）字段里输入标识名，说明在 LDAP 数据库的什么地方开始搜索用户信息。最长可以使用 64 个字符。基本搜索值示例：`cn=Users,dc=raritan,dc=com`。向验证服务器管理员咨询在这些字段输入的适当值。
9. 在 DN of Administrative User（管理用户标识名）字段里输入管理用户标识名（最多 64 个字符）。如果 LDAP 服务器只允许管理员以管理用户身份搜索用户信息，填写此字段。向验证服务器管理员咨询在此字段输入的适当值。管理用户标识名值示例：`cn=Administrator,cn=Users,dc=testradius,dc=com`。**可选**



10. 如果输入了 Distinguished Name for the Administrative User（管理用户标识名），必须输入在远程验证服务器上验证管理用户标识名时所用的密码。在 Secret Phrase（密码）字段里输入密码，在 Confirm Secret Phrase（确认密码）字段里再次输入密码（最长 128 个字符）。



LDAP/安全 LDAP

11. 如果要使用 SSH，选择 Enable Secure LDAP（启用安全 LDAP）复选框。启用 Enable LDAPS Server Certificate Validation（启用 LDAPS 服务器证书验证）复选框。Secure Sockets Layer (SSL) 是允许 Dominion KX II 与 LDAP/LDAPS 服务器通信的加密协议。
12. 默认 Port （端口）是 389。既可以使用标准 LDAP TCP 端口，也可以指定另一个端口。

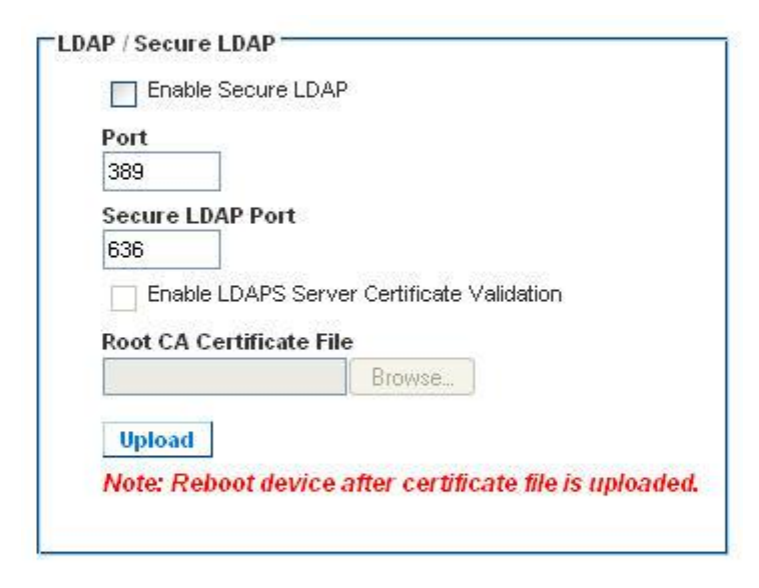


13. 默认 Secure LDAP Port（安全 LDAP 端口）是 636。既可以使用默认端口，也可以指定另一个端口。只有在选择 Enable Secure LDAP（启用安全 LDAP）复选框之后，才启用此字段。
14. 选择 Enable LDAPS Server Certificate Validation（启用 LDAPS 服务器证书验证）复选框，用此前上载的 CA 根证书文件验证服务器提供的证书。如果不想使用此前上载的 CA 根证书文件，不要选择此复选框。如果禁用此功能，表示接受未知认证机构签发的证书。只有在选择 Enable Secure LDAP（启用安全 LDAP）复选框之后，才能使用此复选框。

注意：如果选择 Enable LDAPS Server Certificate Validation（启用 LDAPS 服务器证书验证）选项，除了使用 CA 根证书验证，服务器主机名必须与服务器证书上的公用名相匹配。

---

15. 必要时上载 CA 根证书文件。如果选择 Enable Secure LDAP（启用安全 LDAP）复选框，启用此字段。咨询验证服务器管理员，获取 LDAP 服务器所用的 Base64 编码 X-509 格式的 CA 证书文件。用 Browse（浏览）按钮找到证书文件。如果用新证书取代 LDAP/LDAPS 服务器证书，必须重新启动 Dominion KX II，新证书才生效。

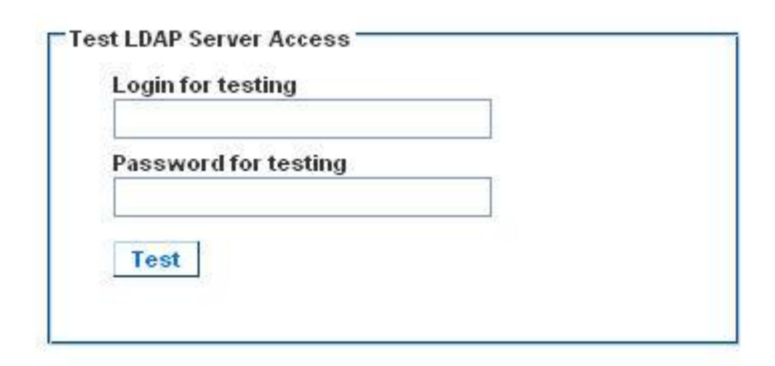


测试 LDAP 服务器访问

16. 由于成功配置 LDAP 服务器和 Dominion KX II 进行远程验证有时很复杂，所以 Dominion KX II 使你能在 Authentication Settings（验证设置）页上测试 LDAP 配置。为了测试 LDAP 配置，分别在 Login for testing（测试登录名）和 Password for testing（测试密码）字段里输入登录名和密码。这是你为访问 Dominion KX II 输入的用户名和密码，LDAP 服务器将用它们验证你的身份。单击 Test（测试）按钮。



在测试完成之后显示一条消息，告诉你测试成功了；如果测试失败，将显示详细错误消息。显示成功结果，或者详细说明失败错误消息。如果测试成功，还显示在 LDAP 服务器上检索的有关测试用户的组信息。



从 Active Directory 服务器返回用户组信息

Dominion KX II 支持用 Active Directory® (AD) 进行用户验证，不要求在 Dominion KX II 本地定义用户。这样，可以在 AD 服务器上单独维护 Active Directory 用户帐号和密码。授权和 AD 用户权限通过标准 Dominion KX II 策略和用户组权限控制和管理，其中策略和用户组权限在本地应用于 AD 用户组。

重要说明：如果你是现有的 Raritan, Inc. 客户，已经通过更改 AD 模式配置了 Active Directory 服务器，Dominion KX II 仍然支持此配置，你不必执行下列操作。参看更新 LDAP 模式，了解如何更新 AD LDAP/LDAPS 模式。

▶ **在 Dominion KX II 上启用 AD 服务器：**

1. 用 Dominion KX II 创建特殊组，给这些组指定适当的权限。例如创建 KVM_Admin 和 KVM_Operator 等组。
2. 在 Active Directory 服务器上创建新组，其名称与在上一步中使用的名称相同。
3. 在 AD 服务器上给 Dominion KX II 用户指定在第二步中创建的组。
4. 在 Dominion KX II 上正确启用和配置 AD 服务器。参看实现 LDAP/LDAPS 远程验证。

重要说明：



- Group Name（组名称）区分大小写。
- Dominion KX II 有下列不能更改或删除的默认组：Admin（管理员）和 <Unknown>（未知）。确认 Active Directory 服务器不使用相同的组名称。
- 如果从 Active Directory 服务器返回的组信息不匹配 Dominion KX II 组配置，Dominion KX II 自动给 <Unknown> 组指定成功验证的用户。
- 如果使用回拨号码，必须输入下列区分大小写的字符串：*msRADIUSCallbackNumber*。
- 根据 Microsoft 的建议，应该使用有用户帐号的 Global Groups（全局组），而不使用 Domain Local Groups（域本地组）。

实现 LDAP/LDAPS 远程验证

Remote Authentication Dial-in User Service (RADIUS) 是供网络访问应用程序使用的 AAA (authentication, authorization, and accounting) 协议。

▶ 使用 RADIUS 验证协议：

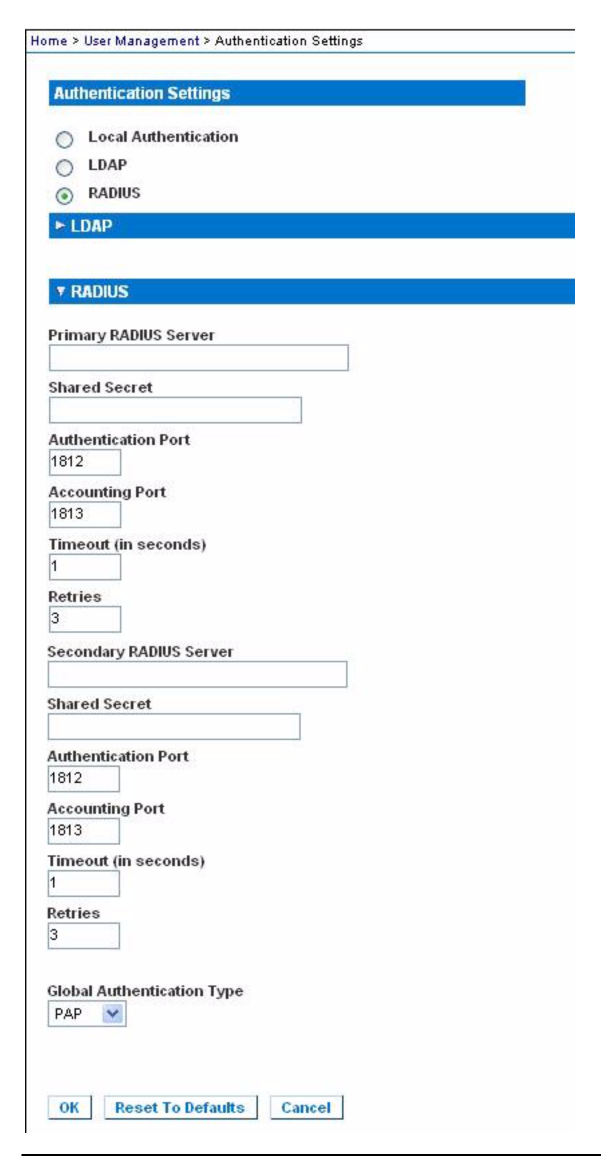
1. 单击 User Management（用户管理）> Authentication Settings（验证设置），打开 Authentication Settings（验证设置）页。
2. 单击 RADIUS 单选按钮启用本页的 RADIUS 部分。
3. 单击 ▶ RADIUS 图标展开本页的 RADIUS 部分。
4. 在 Primary RADIUS Server（主 RADIUS 服务器）字段和 Secondary RADIUS Server（备用 RADIUS 服务器）字段里分别输入主远程验证服务器和备用远程验证服务器的 IP 地址（最多 256 个字符）。
5. 在 Shared Secret（共享密码）字段里输入验证所用的服务器密码（最多 128 个字符）。

   共享密码是 Dominion KX II 和 RADIUS 服务器进行安全通信所要了解的字符串。它从本质上讲是密码。
6. 默认 Authentication Port（验证端口）是 1812，但可以按需要更改端口。
7. 默认 Accounting Port（记帐端口）是 1813，但可以按需要更改端口。
8. Timeout（超时）按秒记录，默认超时是 1 秒，但可以按需要更改超时。

   超时是 Dominion KX II 在发送另一个验证请求之前，等待 RADIUS 服务器做出响应的时间。
9. Retries（重试次数）默认次数是 3 次。

   这是 Dominion KX II 给 RADIUS 服务器发送一个验证请求的次数。

10. 在 Global Authentication Type（全局验证类型）下拉列表上选择选项：
    - PAP — 如果选择 PAP，采用纯文本方式发送密码。PAP 不支持交互操作。在建立连接之后，作为数据包发送用户名和密码，而不是让服务器发送登录提示并等待响应。
    - CHAP — 如果选择 CHAP，服务器随时可以请求验证。CHAP 的安全性比 PAP 高。



注意：同时支持 IPv4 地址和 IPv6 地址。



通过 RADIUS 返回用户组信息

当 RADIUS 验证尝试成功时，Dominion KX II 根据给定用户的组的权限确定他/她的权限。

远程 RADIUS 服务器可以返回作为 RADIUS FILTER-ID 实现的属性，从而提供这些用户组名称。FILTER-ID 应该如下格式化：Raritan:G{*GROUP_NAME*}，其中 *GROUP_NAME* 字符串是用户所属组的名称。

Raritan:G{GROUP_NAME}:D{Dial Back Number}

其中 GROUP_NAME 字符串是用户所属组的名称，Dial Back Number 是与用户帐号关联的号码，Dominion KX II 调制解调器将用此号码回拨该用户帐号。

RADIUS 通信交换规范

Dominion KX II 将下列 RADIUS 属性发送到 RADIUS 服务器：

属性 登录	数据
Access-Request (1)	
NAS-Port-Type (61)	网络连接 VIRTUAL (5)。
NAS-IP-Address (4)	Dominion KX II 的 IP 地址。
User-Name (1)	在登录屏幕上输入的用户名。
Acct-Session-ID (44)	记帐用的会话 ID。
User-Password (2)	加密密码。
Accounting-Request(4)	
Acct-Status (40)	Start(1) — 开始记帐。
NAS-Port-Type (61)	网络连接 VIRTUAL (5)。
NAS-Port (5)	始终是 0。
NAS-IP-Address (4)	Dominion KX II 的 IP 地址。
User-Name (1)	在登录屏幕上输入的用户名。
Acct-Session-ID (44)	记帐用的会话 ID。

属性 登录 退出	数据
Accounting-Request(4)	
Acct-Status (40)	Stop(2) — 停止记帐。
NAS-Port-Type (61)	网络连接 VIRTUAL (5)。
NAS-Port (5)	始终是 0。
NAS-IP-Address (4)	Dominion KX II 的 IP 地址。
User-Name (1)	在登录屏幕上输入的用户名。
Acct-Session-ID (44)	记帐用的会话 ID。



用户验证流程

远程验证流程如下图所示：

User logs in

Is Remote Authentication Enabled?

No

Yes

Is Remote Authentication Server reachable?

No

No

Yes

Is User authenticated in local database?

Is User authenticated in remote database?

Yes

Yes

User allowed

No

User denied

更改密码

▶ 更改密码：

1. 选择 User Management（用户管理）> Change Password（更改密码）。打开 Change Password（更改密码）页。
2. 在 Old Password（旧密码）字段里输入当前密码。
3. 在 New Password（新密码）字段里输入新密码。在 Confirm New Password（确认新密码）字段里再次输入新密码。密码最长为 64 个字符，可以包含英文字母数字字符和特殊字符。
4. 单击 OK（确定）按钮。
5. 显示确认信息，说明密码更改成功。单击 OK（确定）按钮。

---

*注意：如果使用强密码，本页显示强密码格式信息。如要进一步了解密码和强密码，参看*强密码 *(p. 191)*。

Home > User Management > Change Password

Change Password

Old Password

New Password

Confirm New Password

OK Cancel

Ch 8　设备管理

在本章内

网络设置

用 Network Settings（网络设置）页定制 Dominion KX II 网络配置（例如 IP 地址、发现端口和 LAN 接口参数）。

有两个选项可用于设置 IP 配置：

- None（无，默认值）— 这是建议的选项（静态 IP）。由于 Dominion KX II 是网络基础设施的组成部分，很可能不希望 IP 地址频繁变化。此选项使你能设置网络参数。
- DHCP — 如果选择此选项，由 DHCP 服务器自动分配 IP 地址。

▶ 更改网络配置：

1. 选择 Device Settings（设备设置）> Network（网络）。打开 Network Settings（网络设置）页。
2. 更新 Network Basic Settings（基本网络设置）。参看安全基本设置。
3. 更新 LAN Interface Settings（LAN 接口设置）。参看 LAN 接口设置。
4. 单击 OK（确定）按钮设置这些配置。如果所作的更改要求重新启动设备，显示一条重新启动消息。

▶ 复位到出厂前默认值：

- 单击 Reset to Defaults（复位到默认值）。

注意：同时支持 IPv4 地址和 IPv6 地址。

网络基本设置

下列步骤说明如何在 Network Settings（网络设置）页上分配 IP 地址。如要全面了解本页上的所有字段和操作，参看*网络设置* (p. 129)。

1. 选择 Device Settings（设备设置）> Network（网络）。打开 Network Settings（网络设置）页。
2. 给 Dominion KX II 设备指定有意义的设备名称。最长 32 个字母数字字符，可以使用有效特殊字符，但不能使用空格。
3. 在 IPv4 部分输入或选择合适的 IPv4 网络设置：
   a. 必要时输入 IP Address（IP 地址）。默认 IP 地址是 192.168.0.192。
   b. 输入 Subnet Mask（子网掩码）。默认子网掩码是 255.255.255.0。
   c. 如果在 IP Auto Configuration（IP 自动配置）下拉列表上选择了 None（无），输入 Default Gateway（默认网关）。
   d. 如果在 IP Auto Configuration（IP 自动配置）下拉列表上选择了 DHCP，输入 Preferred DHCP Host Name（首选 DHCP 主机名）。
   e. 选择 IP Auto Configuration（IP 自动配置）。有三个选项可供选择：
   - None (Static IP)（无[静态 IP]）— 此选项要求你人工指定网络参数。

     建议你选择此选项，因为 Dominion KX II 是基础设施设备，其 IP 地址不应发生变化。
   - DHCP — 联网计算机（客户机）用 Dynamic Host Configuration Protocol（动态主机配置协议）获取 DHCP 服务器分配的唯一 IP 地址和其他参数。

     如果选择此选项，网络参数由 DHCP 服务器指定。如果使用 DHCP，输入 Preferred host name（首选主机名）（仅限于 DHCP）。最长 63 个字符。
4. 如果要使用 IPv6，在 IPv6 部分输入或选择合适的 IPv6 网络设置：
   a. 选择 IPv6 复选框，激活这部分的字段。
   b. 输入 Global/Unique IP Address（全局/唯一 IP 地址）。这是给 Dominion KX II 分配的 IP 地址。
   c. 输入 Prefix Length（前缀长度）。这是 IPv6 地址使用的位数。
   d. 输入 Gateway IP Address（网关 IP 地址）。
   e. Link-Local IP Address（链路-本地 IP 地址）。自动给设备分配此地址。用于发现邻居，或者在没有路由器时使用。**只读**



f. 域 ID。标识与此地址关联的设备。只读

g. 选择 IP Auto Configuration（IP 自动配置）。有三个选项可供选择：

- None（无）— 如果不想使用自动 IP 配置，而是自己设置 IP 地址（静态 IP），就使用此选项。这是默认选项，建议使用此选项。

  如果给 IP auto configuration（IP 自动配置）选择 None（无），启用下列网络基本设置字段：Global/Unique IP Address（全局/唯一 IP 地址）、Prefix Length（前缀长度）和 Gateway IP Address（网关 IP 地址），你可以人工设置 IP 配置。

- Router Discovery（路由器发现）— 用于选项自动分配 IPv6 地址，这些地址具有 Global（全局）或 Unique Local（唯一本地）意义，超出了 Link Local（链路本地）的意义，仅应用于直接连接的子网。

5. 如果选择了 DHCP，启用了 Obtain DNS Server Address(获取 DNS 服务器地址），就选择 Obtain DNS Server Address Automatically（自动获取 DNS 服务器地址）。在选择 Obtain DNS Server Address Automatically（自动获取 DNS 服务器地址）之后，将使用 DHCP 服务器提供的 DNS 信息。

6. 如果选择了 Use the Following DNS Server Addresses（使用下列 DNS 服务器地址），无论是否选择了 DHCP，均用在此输入的地址连接 DNS 服务器。

   如果选择了 Use the Following DNS Server Addresses（使用下列 DNS 服务器地址）选项，输入下列信息。这些地址分别是主 DNS 地址和备用 DNS 地址，当主 DNS 服务器连接由于中断而断开时，将使用备用 DNS 地址。

   a. Primary DNS Server IP Address（主 DNS 服务器 IP 地址）

   b. Secondary DNS Server IP Address（备用 DNS 服务器 IP 地址）

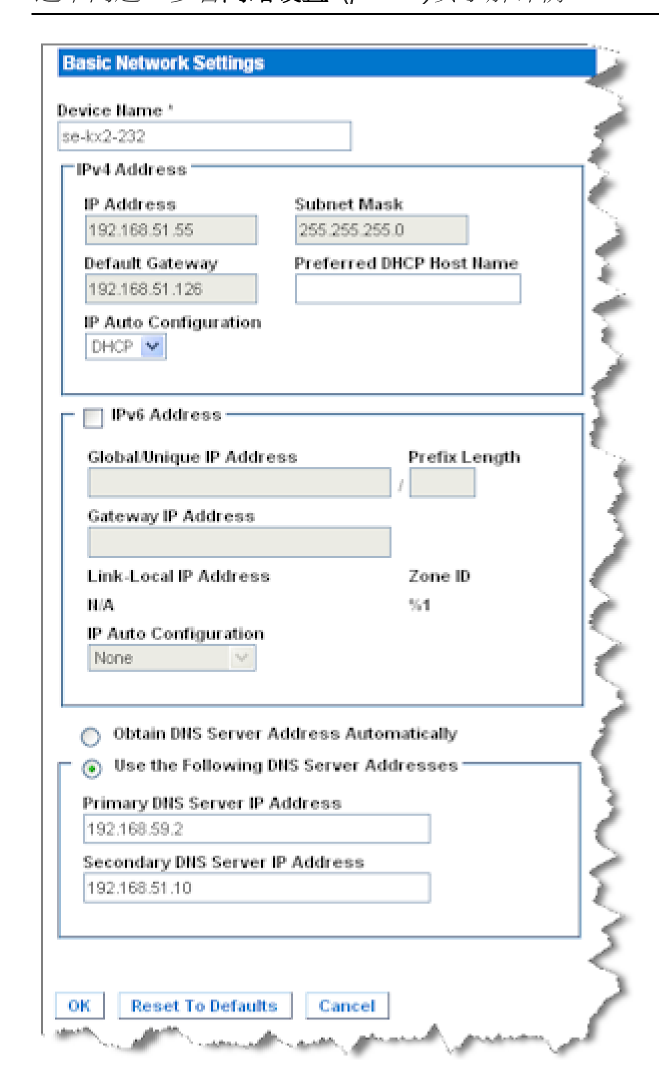
7. 在填写完之后，单击 OK（确定）按钮。现在 Dominion KX II 设备可通过网络访问了。



参看 ***LAN 接口设置*** (p. 132)，了解如何配置 Network Settings（网络设置）页的这个部分。

---

*注意：在某些环境下，默认 LAN Interface Speed & Duplex setting Autodetect (autonegotiator)（LAN 接口速度和全双工设置自动检测[自动协商]）并不能正确设置网络参数，从而引发网络问题。在这些情况下，将 Dominion KX II LAN Interface Speed & Duplex（LAN 接口速度和全双工）设置为 100 Mbps/Full Duplex（全双工）或与网络相适应的其他选项，可以解决这个问题。参看*网络设置 *(p. 129)* *页了解详情。*



LAN 接口设置

1. Current LAN interface parameters（当前 LAN 接口参数）字段显示当前参数设置。



2. 在下列选项上选择 LAN Interface Speed & Duplex（LAN 接口速度和双工）：
   - Autodetect（自动检测，默认选项）
   - 10 Mbps/Half（10 Mbps/半双工）— 两个 LED 指示灯闪烁
   - 10 Mbps/Full（10 Mbps/全双工）— 两个 LED 指示灯闪烁
   - 100 Mbps/Half（100 Mbps/半双工）— 黄色 LED 指示灯闪烁
   - 100 Mbps/Full（100 Mbps/全双工）— 黄色 LED 指示灯闪烁
   - 1000 Mbps/Full（1000 Mbps/全双工）(Gigabit) — 绿色 LED 指示灯闪烁
   - 半双工提供双向通信，但每次只允许一个方向通信，不允许两个方向同时通信。
   - 全双工允许双向同时通信。

注意：在 10 Mbps 速度下进行半双工或全双工通信时，偶尔会出问题。如果出问题，尝试使用另一个速度和双工设置。

参看***网络速度设置*** (p. 275)了解详情。

3. 选择 Enable Automatic Failover（启用自动故障切换）复选框，允许 Dominion KX II 在活动网络端口发生故障时，自动用备用网络端口恢复网络连接。

注意：由于只有在实际发生故障之后才激活故障切换端口，所以 Raritan 建议你不要监视故障切换端口，或者只有在发生故障切换之后才监视该端口。

在启用此选项之后，使用下列两个字段：

- Ping Interval (seconds)（Ping 间隔[秒]）— ping 间隔决定 Dominion KX II 多久检查一次至指定网关的网络路径的状态。默认 ping 间隔是 30 秒。
- Timeout (seconds)（超时[秒]）— 超时决定在进行故障切换之前，指定网关在多长时间内不能通过网络连接访问。

注意：可以根据本地网络的情况，配置最佳 ping 间隔和超时。在设置超时时，应该考虑到至少要发送两个 ping 请求并返回响应。例如假如网络利用率很高，频繁进行故障切换，超时值应该是 ping 间隔的 3-4 倍。

4. 在下列选项中选择 Bandwidth（带宽）：
   - 100 Megabit（2 MB）
   - 10 Megabit（2 MB）



- 5 Megabit（2 MB）
- 2 Megabit（2 MB）
- 512 Kilobit（512 KB）
- 256 Kilobit（256 KB）
- 128 Kilobit（128 KB）

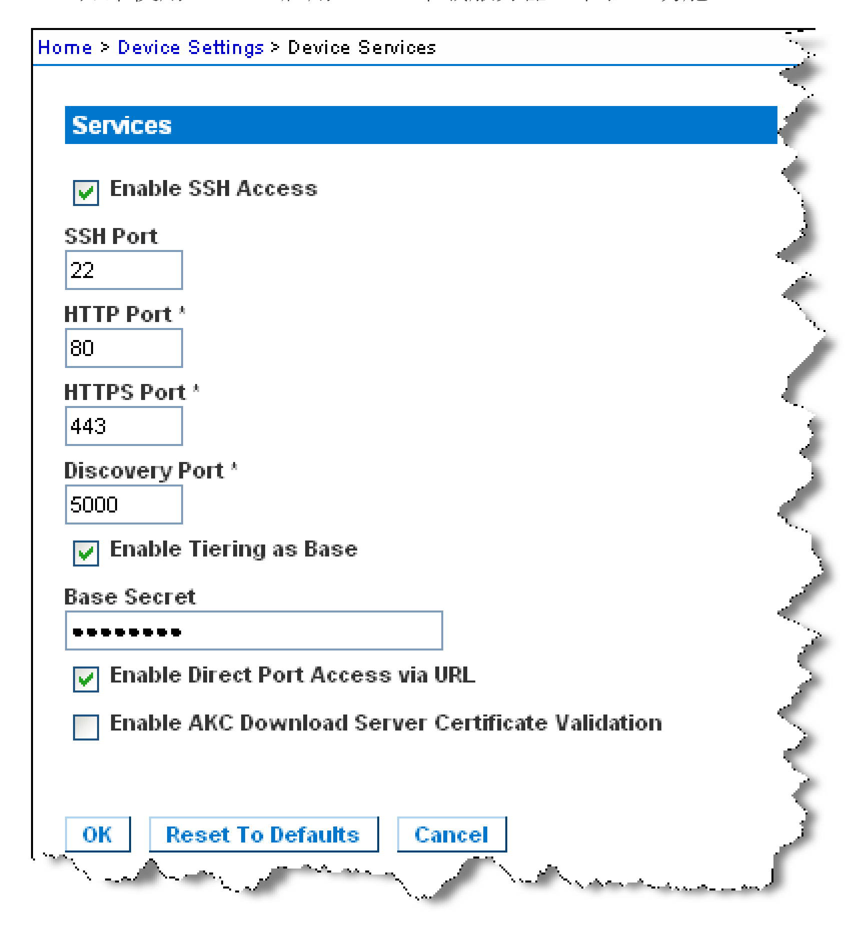
5. 单击 OK（确定）按钮应用 LAN 设置。



设备服务

可以用 Device Services（设备服务）页配置下列功能：

- 启用 SSH 访问。
- 启用基础 Dominion KX II 级联。
- 输入发现端口。
- 启用直接端口访问。
- 如果使用 AKC，启用 AKC 下载服务器证书验证功能。



启用 SSH

启用 SSH 访问，允许管理员通过 SSH v2 应用程序访问 Dominion KX II。

启用 SSH 访问：

1. 选择 Device Settings（设备设置）> Device Services（设备服务）。打开 Device Service Settings（设备服务设置）页。
2. 选择 Enable SSH Access（启用 SSH 访问）。
3. 输入 SSH Port（SSH 端口）信息。标准 SSH TCP 端口号是 22，但可以更改端口号提高安全操作水平。
4. 单击 OK（确定）按钮。

HTTP 和 HTTPS 端口设置

现在可以配置供 Dominion KX II 使用的 HTTP 和/或 HTTPS 端口。 例如如果把默认 HTTP 端口 80 用于其他目的，更改此端口可以确保 Dominion KX II 不尝试使用此端口。

更改 HTTP 和/或 HTTPS 端口设置：

1. 选择 Device Settings（设备设置）> Device Services（设备服务）。打开 Device Service Settings（设备服务设置）页。
2. 在 HTTP Port（HTTP 端口）字段和/或 HTTPS Port（HTTPS 端口）字段里输入新端口。
3. 单击 OK（确定）按钮。

输入发现端口

Dominion KX II 在一个可配置的 TCP 端口上执行发现。默认值是端口 5000，但可以配置使用除 80 和 443 之外的任何 TCP 端口。为了越过防火墙访问 Dominion KX II，防火墙设置必须允许通过默认端口 5000 或在此配置的非默认端口进行双向通信。

启用发现端口：

1. 选择 Device Settings（设备设置）> Device Services（设备服务）。打开 Device Service Settings（设备服务设置）页。
2. 输入 Discovery Port（发现端口）。
3. 单击 OK（确定）按钮。



配置和启用级联

级联功能允许你通过一台基础 Dominion KX II 设备访问多个 Dominion KX II 目标和多个电源条。此功能适用于标准 Dominion KX II 设备、KX2-832 设备和 KX2-864 设备。可以按需要在配置中增删设备，最多两层设备。

在设置设备时，要针对特定配置使用特定的 CIM。 在设置设备时，要针对特定配置使用特定的 CIM。参看***级联 — 目标类型、支持的 CIM 和级联配置*** (p. 139)，了解级联配置可包括的目标、CIM 兼容性和设备配置信息。

在添加级联设备之前，必须针对基础设备和级联设备启用级联。在 Device Settings（设备设置）页上启用基础设备。在 Local Port Settings（本地端口设置）页上启用级联设备。在启用并配置设备之后，Port Access（端口访问）页（***端口访问页*** (p. 41)）显示这些设备。

在将 Dominion KX II 配置为基础设备或级联设备之后，如下显示它们：

- 在 Dominion KX II 界面左面板的 Device Information（设备信息）部分显示 Configured As Base Device（配置为基础设备），表示这是基础设备。
- 在 Dominion KX II 界面左面板的 Device Information（设备信息）部分显示 Configured As Tier Device（配置为级联设备），表示这是级联设备。
- 在级联设备界面左面板的 Connect User（连接用户）下面，显示 Base（基础）表示基础设备。
- 从基础设备到级联端口的目标连接用两个已连接端口表示。

可以通过 Port Access（端口访问）页上的合并端口列表，远程和本地访问基础设备。可以通过级联设备的端口列表，远程访问级联设备。在启用级联之后，在级联设备上不能使用本地访问。

级联还支持用 KVM 切换器在服务器之间来回切换。参看***配置 KVM 切换器*** (p. 156)。

启用级联

用 D2CIM-DVUSB 把基础设备的目标服务器端口连接到级联 Dominion KX II 的本地访问端口。

如果级联设备是 KX2-832 或 KX2-864，把基础设备的目标服务器端口直接连接到级联 KX2-832/KX2-864 的扩展本地端口。

► 启用级联：

1. 在级联基础设备上选择 Device Settings（设备设置）> Device Services（设备服务）。打开 Device Service Settings（设备服务设置）页。



2. 选择 Enable Tiering as Base（作为基础启用级联）。
3. 在 Base Secret（基本密码）字段里输入基础设备和级联设备共用的密码。如果级联设备要验证基础设备，需要此密码。对级联设备输入相同密码。
4. 单击 OK（确定）按钮。
5. 启用级联设备。在级联设备上选择 Device Settings（设备设置）> Local Port Settings（本地端口设置）。
6. 在页面的 Enable Local Ports（启用本地端口）部分选择 Enable Local Port Device Tiering（启用本地端口设备级联）。
7. 在 Tier Secret（级联密码）字段里输入此前在 Device Settings（设备设置）页上输入的基础设备的密码。
8. 单击 OK（确定）按钮。



级联 — 目标类型、支持的 CIM 和级联配置

Blade Chassis（刀片服务器机箱）

可以访问与基础设备直接相连的刀片服务器机箱。

电源控制

可以接通和断开作为级联配置组成部分的目标服务器的电源。在 Port Access（端口访问）页上访问这些目标服务器。

可以利用 Dominion KX II 或 KXII-832 和 KXII-864 型号，通过级联配置访问和控制 Dominion KX II PDU 电源接口。如果目标服务器与电源接口关联，可以在 Port Access（端口访问）页上使用电源控制。目标服务器和 PDU 电源接口关联仅限于那些同一台 Dominion KX II 相连的设备。

Power（电源）页下拉列表显示与基础或级联 Dominion KX II 相连的 PDU，以及所选电源条的统计数据。

还可以使用电源接口级控制。尤其是可以断开当前通电的电源接口，然后再接通电源，但不能给当前断电的电源接口重新通电。

Dominion KX II 到 Dominion KX II 或 KXII-8xx 本地端口配置 — 兼容的 CIM

在配置基础 Dominion KX II 访问和控制附加的 Dominion KX II 或 KXII-832 和 KXII-864 型号，以及 Dominion KX II PDU 和刀片服务器机箱时，下列 CIM 相互兼容。

如果使用 Dominion KX II 和 Dominion KX II 级联的配置，必须使用 D2CIM-DVUSB。如果将 Dominion KX II 用于 KXII-8xx 配置，只能使用扩展本地端口。

如果使用由 Dominion KX II 和 KXII-832 或 KXII-864 构成的配置，每台设备必须运行相同的固件。如果刀片服务器机箱是配置的组成部分，每个刀片服务器机箱算一个目标端口。

级联目标不支持的功能和有限支持的功能

级联目标不支持下列功能：

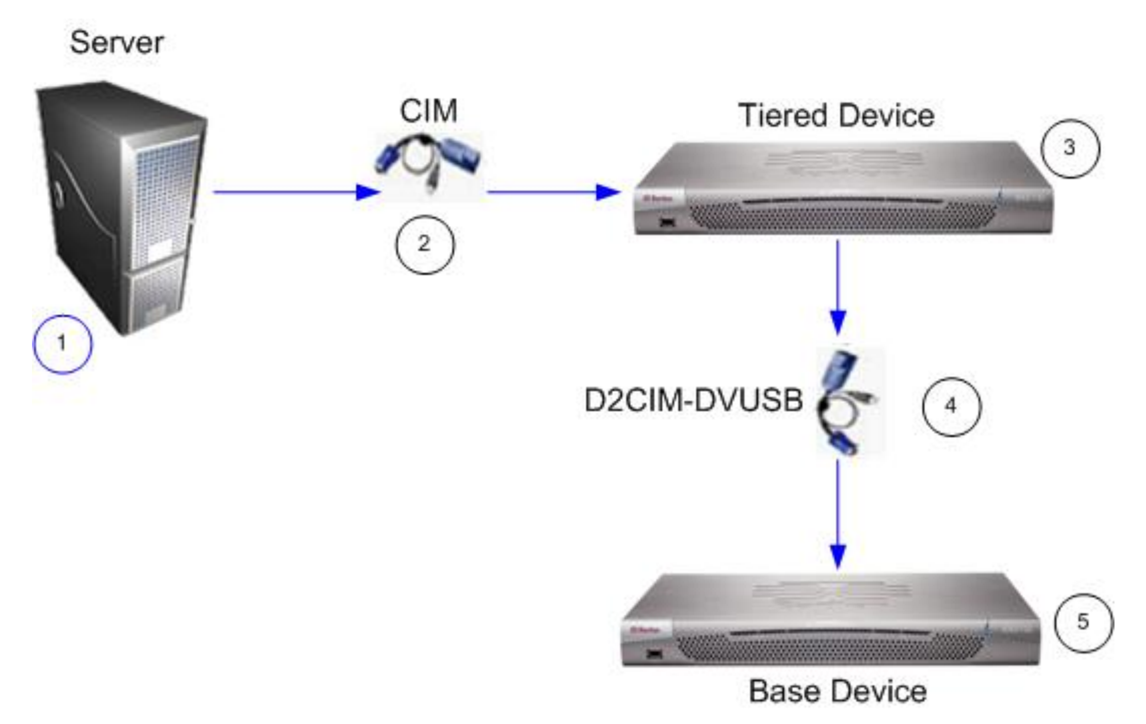
- 级联设备上的刀片服务器机箱
- 级联设备上的智能卡
- 虚拟媒体级联设备
- 用作分层设备的 MCCAT

端口组管理仅限于针对直接连接基础设备的成员创建端口组。

级联配置布线示例

下图说明 Dominion KX II 级联设备和 Dominion KX II 基础设备之间的布线配置。 用 D2CIM-DVUSB 把基础设备的目标服务器端口连接到级联 Dominion KX II 的本地访问端口。

如果级联设备是 KX2-832 或 KX2-864，把基础设备的目标服务器端口直接连接到级联 KX2-832/KX2-864 的扩展本地端口。



图示符号	
1	目标服务器
2	用于连接目标服务器和 Dominion KX II 级联设备的 CIM
3	Dominion KX II 级联设备
4	用于连接 Dominion KX II 级联设备和 Dominion KX II 基础设备的 D2CIM-DVUSB CIM
5	Dominion KX II 基础设备



启用直接端口访问

直接端口访问允许用户绕过设备的 Login（登录）对话框和 Port Access（端口访问）页。此功能还允许用户在 URL 不包含用户名和密码的情况下，直接输入用户名和密码访问目标服务器。

下面说明有关直接端口访问的重要 URL 信息：

如果使用 VKC 和直接端口访问：

- https://IPaddress/dpa.asp?username=username&password=password&port=port number

如果使用 AKC 和直接端口访问：

- https://IPaddress/dpa.asp?username=username&password=password&port=port number&client=akc

其中：

- username 和 password 是可选的。如果不使用 username 和 password，将显示登录屏幕，用户在验证之后直接连接目标服务器。
- port 可以是端口号或端口名称。如果使用端口名称，名称必须是唯一的，否则系统报告出错。如果忽略端口，系统报告错误。
- 对于刀片服务器机箱，port 是指定的 <port number>'-'<slot number>。例如 1-2 表示刀片服务器机箱连接端口 1、插槽 2。
- Client=akc 是可选的，除非你使用 AKC 客户机。如果没有 client=akc，使用 VKC 客户机。

▶ 启用直接端口访问：

1. 选择 Device Settings（设备设置）> Device Services（设备服务）。打开 Device Service Settings（设备服务设置）页。
2. 如果希望用户通过 URL 传递必要参数，在 Dominion KX II 上直接访问目标服务器，选择 Enable Direct Port Access via URL（启用通过 URL 直接端口访问）。
3. 单击 OK（确定）按钮。

启用 AKC 下载服务器证书验证

如果使用 AKC 客户机，可以选择使用 Enable AKC Download Server Certificate Validation（启用 AKC 下载服务器证书验证）功能，也可以选择不使用此功能。

选项 1：Do Not Enable AKC Download Server Certificate Validation（不启用 AKC 下载服务器证书验证，默认设置）

如果不启用 AKC 下载服务器证书验证，所有 KX II 用户和 CC-SG Bookmark and Access Client 用户必须：

- 确保当前不阻止来自正在访问的设备的 IP 地址的 cookies。
- Windows Vista、Windows 7 和 Windows 2008 服务器用户应该确保正在访问的设备的 IP 地址位于浏览器的 Trusted Sites Zone（信任网站区域），在访问设备时不在 Protected Mode（保护模式）下。

选项 2：Enable AKC Download Server Certificate Validation（启用 AKC 下载服务器证书验证）

如果启用 AKC 下载服务器证书验证：

- 管理员必须把有效证书上载到 Dominion KX II 上，或者在 Dominion KX II 上创建一个自签名证书。证书必须有有效主机名。
- 每个用户必须把 CA 证书（或自签名证书）添加到浏览器的 Trusted Root CA 仓库。

▶ 在使用 Windows Vista® 和 Windows 7® 操作系统时安装自签名证书：

1. 把 Dominion KX II IP 地址加入 Trusted Site zone（信任网站区域），确保关闭 Protected Mode（保护模式）。
2. 用 Dominion KX II IP 地址作为 URL 启动 Internet Explorer®。显示一条证书错误消息。
3. 选择 View Certificates（查看证书）。
4. 单击 General（常规）选项卡上的 Install Certificate（安装证书）。然后把证书安装在信任根 CA 仓库里。
5. 在安装证书之后，可以把 Dominion KX II IP 从 Trusted Site zone（信任网站区域）删除掉。

▶ 启用 AKC 下载服务器证书验证：

1. 选择 Device Settings（设备设置）> Device Services（设备服务）。打开 Device Service Settings（设备服务设置）页。



2. 选择 Enable AKC Download Server Certificate Validation（启用 AKC 下载服务器证书验证）复选框，也可以继续禁用此功能（默认）。
3. 单击 OK（确定）按钮。

配置调制解调器设置

▶ **配置调制解调器设置：**

1. 单击 Device Settings（设备设置）> Modem Settings（调制解调器设置），打开 Modem Settings（调制解调器设置）页。
2. 选择 Enable Modem(启用调制解调器)复选框。这将启用 Serial Line Speed（串行线路速度）字段和 Modem Init String（调制解调器初始化字符串）字段。
3. 调制解调器 Serial Line Speed（串行线路速度）设置为 115200。只读
4. 在 Modem Init String（调制解调器初始化字符串）字段里输入初始调制解调器字符串。如果调制解调器字符串保留空白，默认给调制解调器发送下列字符串：ATZ OK AT OK。

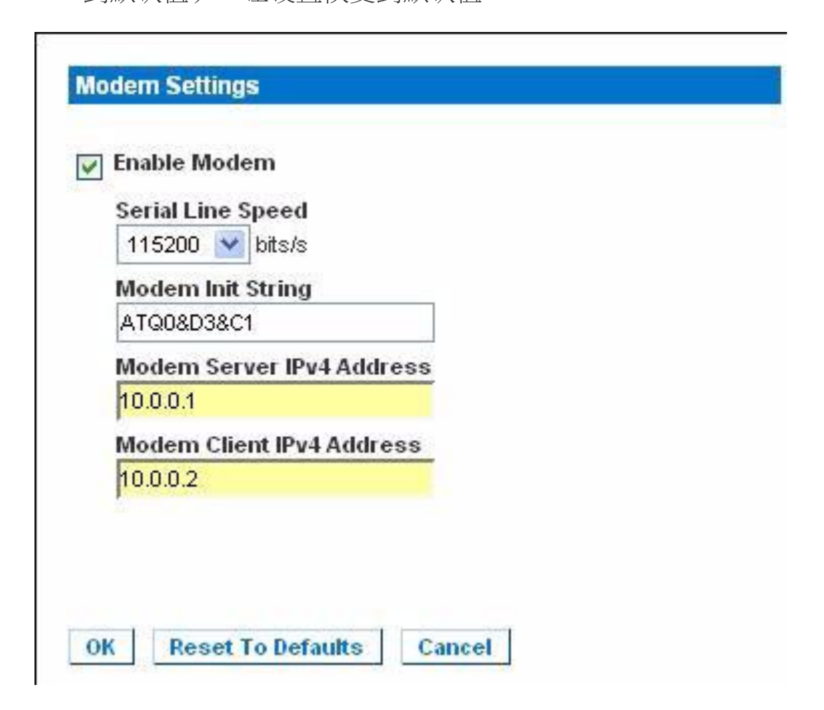
   此信息用于配置调制解调器设置。 由于不同的调制解调器采用不同的方法设置这些值，所以本文不规定如何设置这些值，用户更希望调制解调器创建更适合调制解调器的字符串。

   - 调制解调器设置：
   - 启用 RTS/CTS 流控制。
   - 在收到 RTS 请求之后将数据发送到计算机。
   - 应配置 CTS，只有在流控制要求时才丢弃 CTS。
   - 应配置 DTR，在 DTR 触发时调制解调器复位。
   - 应将 DSR 配置为常开。
   - 应将 DCD 配置为在检测到载波信号之后启用。（也就是说，只有在与远程设备建立调制解调器连接之后，才应启用 DCD。）
5. 在 Modem Server IPv4 Address（调制解调器服务器 IPv4 地址）字段里输入 IPv4 调制解调器服务器地址，在 Modem Client IPv4 Address（调制解调器客户机 IPv4 地址）字段里输入 IPv4 调制解调器客户机地址。

注意：调制解调器客户机 IP 地址和调制解调器服务器 IP 地址必须在同一个子网上，不能与 KX LAN 子网重叠。



6. 单击 OK（确定）按钮提交更改，或者单击 Reset to Defaults（复位到默认值），让设置恢复到默认值。



参看***通过认证的调制解调器*** (p. 267)，了解与 Dominion KX II 一起使用的通过认证的调制解调器。参看 **KVM 和串行访问客户机指南**中的"在 MPC 上创建、修改和删除配置文件 — 第二代设备"，了解在通过调制解调器连接 Dominion KX II 时，如何配置使性能最佳的设置。

注意：调制解调器不支持直接访问 Dominion KX II HTML 界面。必须使用独立 MPC，通过调制解调器访问 Dominion KX II。

配置日期/时间设置

用 Date/Time Settings（日期/时间设置）页给 Dominion KX II 指定日期和时间。有两种方法配置日期和时间：

- 人工设置日期和时间。
- 使日期和时间与 Network Time Protocol (NTP) 服务器同步。

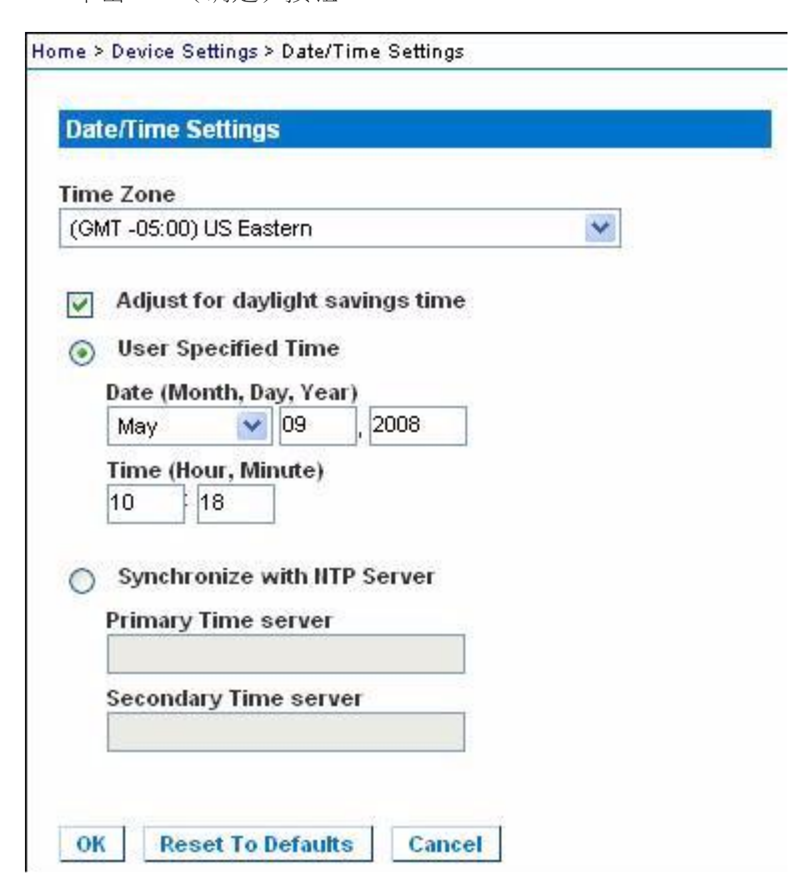
▶ 设置日期和时间：

1. 选择 Device Settings（设备设置）> Date/Time（日期/时间）。打开 Date/Time Settings（日期/时间设置）页。
2. 在 Time Zone（时区）下拉列表上选择你所在的时区。



3. 如要调节夏令时，选择 Adjust for daylight savings time（调节夏令时）复选框。
4. 选择日期和时间设置方法：
   - User Specified Time（用户指定时间）— 选择此选项人工输入日期和时间。

     针对 User Specified Time（用户指定时间）选项输入日期和时间。时间使用 hh:mm 格式（使用 24 小时时钟）。
   - Synchronize with NTP Server（与 NTP 服务器同步）— 选择此选项使日期和时间与 Network Time Protocol (NTP) 服务器同步。
5. 对于 Synchronize with NTP Server（与 NTP 服务器同步）选项：
   a. 输入 Primary Time Server（主时间服务器）的 IP 地址。
   b. 输入 Secondary Time Server（备用时间服务器）的 IP 地址。**可选**
6. 单击 OK（确定）按钮。



注意：同时支持 IPv4 地址和 IPv6 地址。



事件管理

Dominion KX II 事件管理功能提供一组屏幕，用于启用和禁用系统事件至 SNMP 管理器、系统日志和审计日志的分发。这些事件分成不同的类别，你可以确定要将每个事件发送到一个目的地还是几个目的地。

配置事件管理 — 设置

SNMP 配置

Simple Network Management Protocol (SNMP) 是用于网络管理和网络设备及其功能监视的协议。Dominion KX II 通过事件管理提供 SNMP 代理支持。

配置 SNMP（启用 SNMP 日志）：

1. 选择 Device Settings（设备设置）> Event Management（事件管理）— Settings（设置）。打开 Event Management - Settings（事件管理 — 设置）页。
2. 选择 SNMP Logging Enabled（启用 SNMP 日志）。这将启用其他 SNMP 字段。
3. 在 Name（名称）字段、Contact（联系人）字段和 Location（位置）字段里分别输入 Dominion KX II 控制台界面显示的 SNMP 代理名称（即设备名称）、与此设备相关的联系人姓名和 Dominion 设备的物理位置。
4. 输入 Agent Community String（代理公用串，设备字符串）。SNMP 公用名是设备和运行 SNMP 的工作站所属的组，有助于定义要将信息发送到哪里。公用名用于标识该组。SNMP 设备或代理可能属于多个 SNMP 公用名。
5. 用 Type（类型）下拉列表指定公用名是 Read-Only（只读）还是 Read/Write（读写）。
6. 指定 SNMP 管理器的 Destination IP/Host Name（目标 IP/主机名）、Port #（端口号）和 Community（公用名），最多可以配置五个 SNMP 管理器。
7. 单击 Click here（单击这里）查看 Dominion SNMP MIB 链接，即可访问 SNMP 管理信息库。
8. 单击 OK（确定）按钮。



▶ 配置系统日志（启用系统日志转发）：

1. 选择 Enable Syslog Forwarding（启用系统日志转发），将设备消息记录到远程系统日志服务器上。
2. 在 IP Address（IP 地址）字段里输入系统日志服务器的 IP 地址/主机名。
3. 单击 OK（确定）按钮。

▶ 复位到出厂前默认值：

- 单击 Reset to Defaults（复位到默认值）。

注意：同时支持 IPv4 地址和 IPv6 地址。

注意：主机名 IPv6 地址长度不能超过 80 个字符。

Home > Device Settings > Event Management - Settings

SNMP Configuration

☑ SNMP Logging Enabled

Name
DominionKX

Contact

Location

Agent Community String

Type
Read-Only

Destination IP/Hostname	Port #	Community
	162	public
	162	public
	162	public
	162	public
	162	public

Click here to view the Dominion KX II SNMP MIB

SysLog Configuration

☐ Enable Syslog Forwarding

IP Address/Host Name

OK | Reset To Defaults | Cancel

事件管理 — 目的地

如果启用了系统事件，系统事件可以生成 SNMP 通知事件（陷阱），也可以记录到系统日志和审计日志里。用 Event Management - Destinations（事件管理 — 目的地）页选择要跟踪的系统事件，以及要将这些信息发送到哪里。

注意：只有在选择了 SNMP Logging Enabled（启用 SNMP 日志）选项之后，才会生成 SNMP 陷阱。只有在选择了 Enable Syslog Forwarding（启用系统日志转发）选项之后，才会生成系统日志事件。两个选项均在 Event Management - Settings（事件管理 — 目的地）页上。参看配置事件管理 — 设置。

▶ 选择事件及其目的地：

1. 选择 Device Settings（设备设置）> Event Management - Destinations（事件管理 — 目的地）。打开 Event Management - Destinations（事件管理 — 目的地）页。

   系统事件按 Device Operation（设备操作）、Device Management（设备管理）、Security（安全）、User Activity（用户活动）和 User Group Administration（用户组管理）分成不同的类别。

2. 选择你要启用或禁用的事件对应的复选框，以及信息目的地对应的复选框。

   提示：选择或取消相应的类别复选框，即可启用或禁用整个类别。



3. 单击 OK（确定）按钮。

Home > Device Settings > Event Management - Destinations Logout

Event Management - Destinations

Note: SNMP traps will only be generated if the "SNMP Logging Enabled" option is checked. Similarly, Syslog events will only be generated if the "Enable Syslog Forwarding" option is checked. These options can be found on the "Event Management - Settings" page on the Device Settings menu.

Category	Event	SNMP	Syslog	Audit Log
Device Operation		✓	✓	✓
	System Startup	✓	✓	✓
	System Shutdown	✓	✓	✓
	Power Supply Status Changed	✓	✓	✓
	Powerstrip Outlet Status Changed	✓	✓	✓
	Network Parameter Changed	✓	✓	✓
	Port Status Changed	✓	✓	✓
	Network Failure			✓
	Ethernet Failover	✓	✓	✓
Device Management		✓	✓	✓
	FactoryReset	✓	✓	✓
	Begin CC Control	✓	✓	✓
	End CC Control	✓	✓	✓
	Device Update Started	✓	✓	✓
	Device Update Completed	✓	✓	✓
	Device Update Failed	✓	✓	✓
	Firmware Update Failed	✓	✓	✓
	Firmware File Discarded	✓	✓	✓
	Firmware Validation Failed	✓	✓	✓
	Configuration Backed Up	✓	✓	✓
	Configuration Restored	✓	✓	✓
	Port Connection Denied	✓	✓	✓
Security		✓	✓	✓
	Password Settings Changed	✓	✓	✓
	Login Failed	✓	✓	✓
	Password Changed	✓	✓	✓
	User Blocked		✓	✓
User Activity		✓	✓	✓
	Port Connected	✓	✓	✓
	Port Disconnected	✓	✓	✓

▶ 复位到出厂前默认值：

- 单击 Reset to Defaults（复位到默认值）。

警告：在使用基于 UDP 的 SNMP 陷阱时，在重新启动 Dominion KX II 之后，Dominion KX II 和相连的路由器可能会不同步，致使重新启动操作不能完成 SNMP 陷阱记录。

SNMP 代理配置

符合 SNMP 规范的设备称为代理，将有关自己的信息存储在管理信息库 (MIB) 里，并将这些数据返回给 SNMP 管理器。用 Event Logging（事件日志）页配置 Dominion KX II（SNMP 代理）和 SNMP 管理器之间的 SNMP 连接。

SNMP 陷阱配置

在满足一个或多个条件时，SNMP 可以发送陷阱或通知，将此事通知管理员。下表列出 Dominion KX II SNMP 陷阱：

陷阱名称	说明
bladeChassisCommError	检测到与此端口相连的刀片服务器机箱发生通信错误。 *注意：KX II-101 不支持。*
configBackup	设备配置已备份。
configRestore	设备配置已恢复。
deviceUpdateFailed	设备更新失败。
deviceUpgradeCompleted	Dominion KX II 用 RFP 文件完成了更新。
deviceUpgradeStarted	Dominion KX II 开始用 RFP 文件更新。
factoryReset	设备已被复位到出厂前默认设置。
firmwareFileDiscarded	固件文件被丢弃。
firmwareUpdateFailed	固件更新失败。
firmwareValidationFailed	固件验证失败。
groupAdded	给 Dominion KX II 系统添加了一个组。
groupDeleted	在系统里删除了一个组。
groupModified	修改了一个组。
ipConflictDetected	检测到 IP 地址冲突。



陷阱名称	说明
ipConflictResolved	解决了 IP 地址冲突。
networkFailure	产品的 Ethernet 接口不再通过网络通信。
networkParameterChanged	更改了网络参数。
passwordSettingsChanged	更改了强密码设置。
portConnect	此前验证的用户开始了 KVM 会话。
portConnectionDenied	连接目标服务器端口被拒绝。
portDisconnect	参与 KVM 会话的一个用户正确关闭了会话。
portStatusChange	端口不可用。
powerNotification	电源接口状态通知：1=活动, 0=闲置。
powerOutletNotification	电源条设备电源接口状态通知。
rebootCompleted	Dominion KX II 重新启动完毕。
rebootStarted	Dominion KX II 已开始采用系统重新通电或操作系统热启动方式重新启动。
securityViolation	违反安全。
startCCManagement	设备受 CommandCenter 管理。
stopCCManagement	设备不再受 CommandCenter 管理。
userAdded	给系统添加了一个用户。
userAuthenticationFailure	用户尝试用错误用户名和/或密码登录。
userConnectionLost	有活动会话的用户遇到异常会话终止现象。
userDeleted	一个用户帐号被删除了。
userForcedLogout	管理员强制用户退出了。
userLogin	用户成功登录 Dominion KX II 并通过验证。
userLogout	用户采用正确方法成功退出 Dominion KX II。
userModified	一个用户帐号被修改了。
userPasswordChanged	如果修改设备的任何用户的密码，就触发此事件。
userSessionTimeout	有活动会话的用户由于超时而终止会话。
userUploadedCertificate	用户上载了 SSL 证书。
vmImageConnected	用户尝试在使用虚拟媒体的目标服务器上安装设备或镜像文件。对于每个设备/镜像文件映射（安装）尝试，均生成此事件。

陷阱名称	说明
vmImageDisconnected	用户尝试在使用虚拟媒体的目标服务器上卸载设备或镜像文件。

电源设置

Dominion KX II 有两个电源，可以自动检测这些电源的状态并发出通知。在 Power Supply Setup（电源设置）页上指定是要使用一个电源，还是使用两个电源。正确配置电源，确保在一个电源发生故障时，Dominion KX II 能发送相应的通知。例如假如电源 1 发生故障，设备面板上的电源 LED 指示灯变成红色。

► 针对使用的电源启用自动检测：

1. 选择 Device Settings（设备设置）> Power Supply Setup（电源设置）。打开 Power Supply Setup（电源设置）页。



2. 如果将电源输入线插入电源 1（设备背面最左边的电源），选择 PowerIn1 Auto Detect（电源输入 1 自动检测）选项。
3. 如果将电源输入线插入电源 2（设备背面最右边的电源），选择 PowerIn2 Auto Detect（电源输入 2 自动检测）选项。
4. 单击 OK（确定）按钮。



注意：如果选择任一个复选框，但实际上并没有连接电源输入，设备面板上的电源 LED 指示灯变成红色。

关闭自动检测：

- 取消相应电源对应的复选框。

复位到出厂前默认值：

- 单击 Reset to Defaults（复位到默认值）按钮。

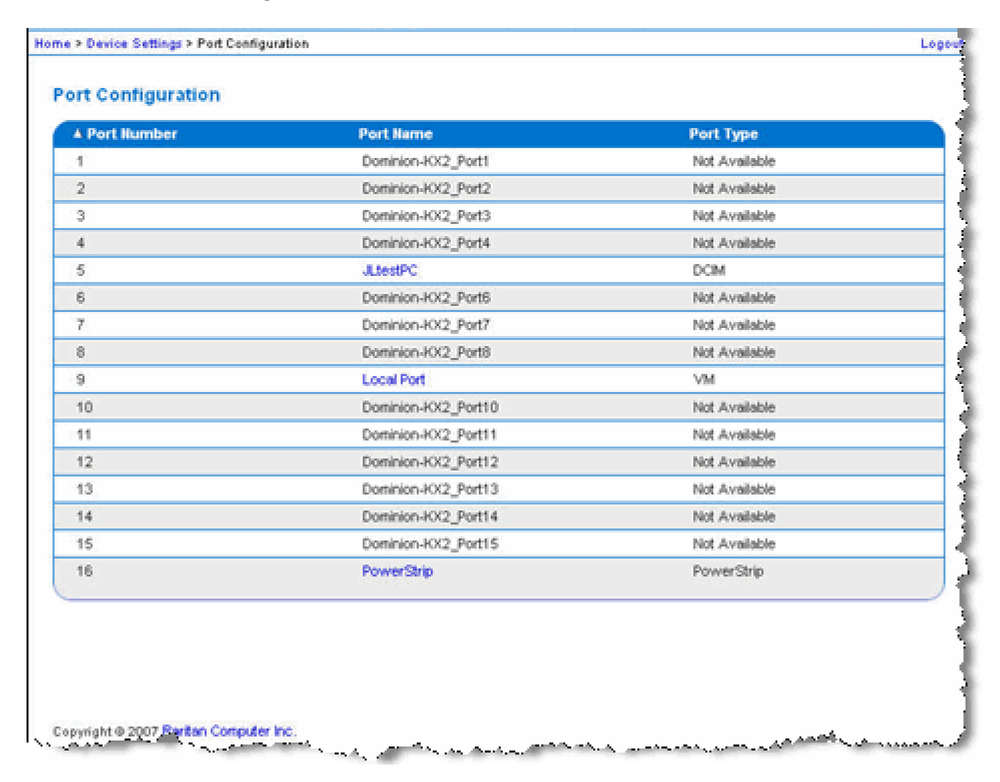
注意：Dominion KX II 不向 CommandCenter 报告电源状态。但是，Dominion I（第一代）向 CommandCenter 报告电源状态。

配置端口

Port Configuration(端口配置)页显示 Domionion KX II 端口列表。与 KVM 目标服务器（刀片服务器和标准服务器）和电源条相连的端口用蓝色显示，可以编辑。对于没有插入 CIM 的端口或 CIM 名称为空白的端口，指定默认端口名称 Dominion-KX2_Port#，其中 Port# 是 Dominion KX II 物理端口编号。

访问端口配置：

1. 选择 Device Settings（设备设置）> Port Configuration（端口配置）。打开 Port Configuration（端口配置）页。



▲ Port Number	Port Name	Port Type
1	Dominion-KX2_Port1	Not Available
2	Dominion-KX2_Port2	Not Available
3	Dominion-KX2_Port3	Not Available
4	Dominion-KX2_Port4	Not Available
5	JLtestPC	DCIM
6	Dominion-KX2_Port6	Not Available
7	Dominion-KX2_Port7	Not Available
8	Dominion-KX2_Port8	Not Available
9	Local Port	VM
10	Dominion-KX2_Port10	Not Available
11	Dominion-KX2_Port11	Not Available
12	Dominion-KX2_Port12	Not Available
13	Dominion-KX2_Port13	Not Available
14	Dominion-KX2_Port14	Not Available
15	Dominion-KX2_Port15	Not Available
16	PowerStrip	PowerStrip

本页最初按端口号顺序显示，但可以单击列标题按任何字段排序。

- Port Number（端口号）— 从 1 到 Dominion KX II 设备的总端口数进行编号。
- Port Name（端口名称）— 给端口指定的名称。用黑色显示的端口名称表示不能更改名称，不能编辑端口；用蓝色显示的端口名称可以编辑。

注意：切勿在 Port (CIM) Name（端口 (CIM) 名称）中使用撇号。



- 端口类型

端口类型	说明
DCIM	Dominion CIM
Not Available（不可用）	没有插 CIM
PCIM	Paragon CIM
PowerStrip（电源条）	电源 CIM
VM（虚拟媒体）	虚拟媒体 CIM（D2CIM-VUSB 和 D2CIM-DVUSB）
Blade Chassis（刀片服务器机箱）	刀片服务器机箱和与该机箱关联的刀片服务器（按分层顺序显示）

2. 单击要编辑的端口的端口名称。
   - 对于 KVM 端口，打开 Port（端口）页。可以在本页上命名端口，创建电源关联。
   - 对于电源条，打开电源条对应的 Port（端口）页。可以在本页上命名电源条及其电源接口。

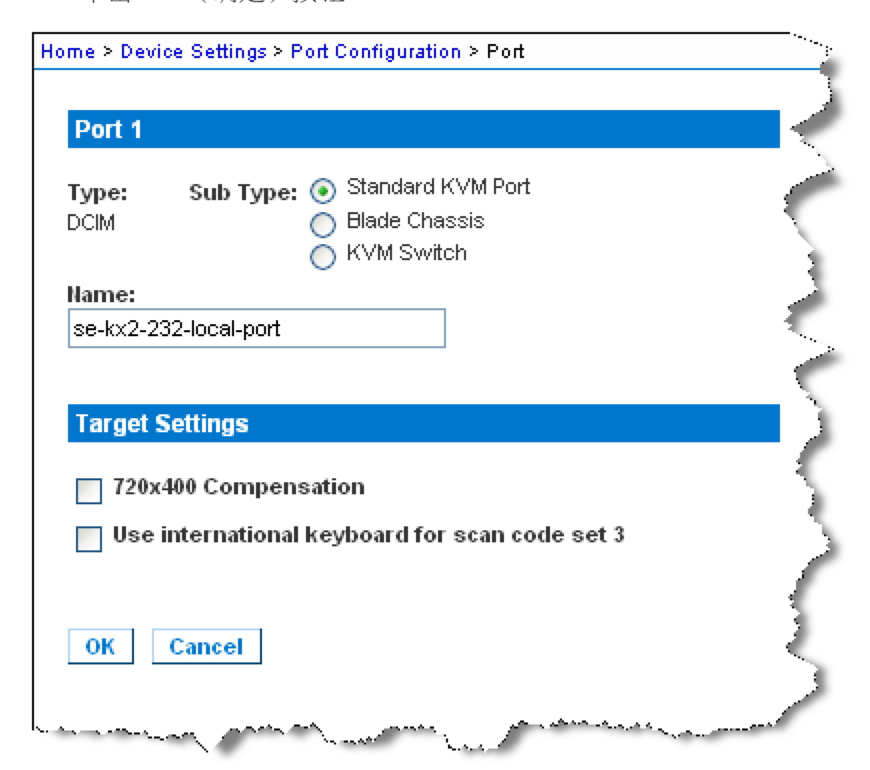
配置标准目标服务器

▶ 命名目标服务器：

1. 连接所有目标服务器（如果尚未连接）。参看***第三步：连接设备*** (p. 26)，了解如何连接设备。
2. 选择 Device Settings（设备设置）> Port Configuration（端口配置）。打开 Port Configuration（端口配置）页。
3. 单击要重新命名的目标服务器的 Port Name（端口名称）。打开 Port（端口）页。
4. 给与该端口相连的服务器指定一个名称。名称最长为 32 个字符，可以使用字母数字字符和特殊字符。
5. 选择 Standard KVM Port（标准 KVM 端口）作为端口子类型。
6. 如果在目标监视器使用此分辨率时显示有问题，在 Target Settings（目标设置）部分选择 720x400 Compensation（720x400 补偿）。
7. 如果用 DCIM-PS2 连接目标，且需要使用扫描代码集 3 和国际键盘，选择 Use international keyboard for scan code set 3（把国际键盘用于扫描代码集 3）。



8. 单击 OK（确定）按钮。



配置 KVM 切换器

Dominion KX II 还支持用热键切换目标服务器。除了用热键切换标准服务器，刀片服务器机箱和级联配置还支持 KVM 切换。

▶ 配置 KVM 切换器：

1. 选择 Device Settings（设备设置）> Port Configuration（端口配置）。打开 Port Configuration（端口配置）页。
2. 单击要重新命名的目标服务器的 Port Name（端口名称）。打开 Port（端口）页。
3. 选择 KVM Switch（KVM 切换器）。
4. 选择 KVM Switch Model（KVM 切换器型号）。

注意：下拉列表只显示一台切换器。

5. 选择 KVM Switch Hot Key Sequence（KVM 切换热键）。
6. 输入 Maximum Number of Target Ports（最大目标端口号）(2-32)。
7. 在 KVM Switch Name（KVM 切换器名称）字段里输入此端口连接的名称。



8. 激活 KVM 切换热键要应用的目标服务器。选择每个端口对应的 Active（活动），说明这些端口连接了目标服务器。
9. 可以在本页的 KVM Managed Links（KVM 管理链接）部分配置至可用的网络浏览器接口的连接。
   a. Active（活动）— 如在配置此链接之后要激活它，选择 Active（活动）复选框。如不选择此复选框，链接保持闲置状态。即使不选择 Active（活动），仍然可以在链接字段里输入并保存信息。一旦选择 Active（活动），就必须填写 URL 字段。用户名字段和密码字段是可选的，取决于是否需要单点登录。
   b. URL Name（URL 名称）— 输入接口 URL。
   c. Username（用户名）— 输入访问接口所用的用户名。
   d. Password（密码）— 输入访问接口所用的密码。
   e. Username（用户名）字段 — 输入要在 URL 中使用的用户名参数。例如 *username*=admin，其中 *username* 是用户名字段。
   f. Password（密码）字段 — 输入要在 URL 中使用的密码参数。例如 *password*=raritan，其中 *password* 是密码字段。
10. 单击 OK（确定）按钮。

▶ 更改 KVM 切换器端口或 URL 的活动状态：

1. 选择 Device Settings（设备设置）> Port Configuration（端口配置）。打开 Port Configuration（端口配置）页。
2. 单击要重新命名的目标服务器的 Port Name（端口名称）。打开 Port（端口）页。
3. 取消 KVM 切换器目标端口或 URL 旁边的 Active（活动）复选框，更改其活动状态。
4. 单击 OK（确定）按钮。

配置接入的电源条（机架式 PDU）

可以利用 KX II 把电源条(机架式 PDU)连接到 KX II 端口。在 KX II Port Configuration（KX II 端口配置）页上进行 KX II 电源条配置。

连接电源条

利用 D2CIM-PWR CIM 把 Raritan PX 系列电源条连接到 KX II。

连接电源条：

1. 把 D2CIM-PWR 的 RJ-45 连接器（公头）插入电源条串行端口上的 RJ-45 连接器（母头）。
2. 使用直通五类电缆把 D2CIM-PWR 的 RJ-45 连接器(母头)插入 KX II 的可用系统端口连接器（母头）。
3. 用交流电源线连接目标服务器和可用的电源条接口。
4. 将电源条连接到交流电源。
5. 接通设备电源。





命名 KX II 的电源条（电源条端口页）

注意：可以命名 PX 和 KX II 的 PX 电源条。

在 Port Configuration（端口配置）页上选择一个与 Raritan 远程电源条相连的端口时，打开 Port（端口）页。自动填充 Type（类型）字段和 Name（名称）字段。

注意：不能更改 CIM 类型。

显示电源条上每个电源接口的下列信息：[Outlet（电源接口）] Number（编号）、Name（名称）和 Port Association（端口关联）。

用此页命名电源条及其接口。所有名称最长为 32 个字母数字字符，可以包含特殊字符。

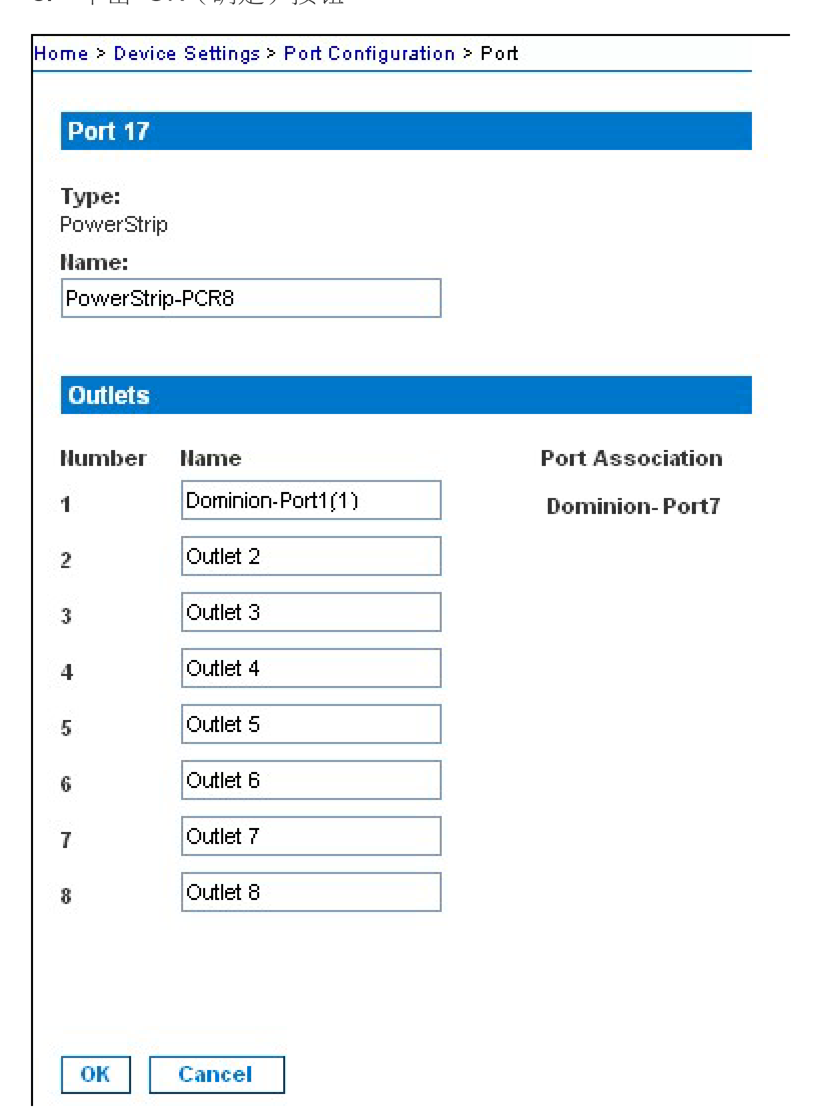
注意：如果电源条与目标服务器（端口）关联，即使你给电源接口指定了另一个名称，也用目标服务器名称取代电源接口名称。

► 命名电源条（和电源接口）：

注意：CommandCenter Service Gateway 不识别有空格的电源条名称。

1. 输入电源条的 Name（名称）（如有必要）。
2. 根据需要更改 [Outlet（电源接口）] Name（名称）。（电源接口名称默认为 outlet #。）

3. 单击 OK（确定）按钮。


Home > Device Settings > Port Configuration > Port
Port 17
Type:
PowerStrip
Name:
PowerStrip-PCR8
Outlets
Number
Name
Port Association
1
Dominion-Port1(1)
Dominion- Port7
2
Outlet 2
3
Outlet 3
4
Outlet 4
5
Outlet 5
6
Outlet 6
7
Outlet 7
8
Outlet 8
OK
Cancel


Raritan.

在 KX II 上使电源接口与目标服务器关联

单击 Port Configuration（端口配置）页上的一个端口，打开 Port（端口）页。可以在本页上创建电源关联，将端口名称更改为更具说明性的名称，更新目标服务器设置(如果使用 D2CIM-VUSB CIM)。自动填充 (CIM) Type(类型)和 (Port（端口）) Name（名称）字段；注意不能更改 CIM 类型。

一台服务器最多可以有四个电源插头，你可以使每个电源插头与不同的电源条关联。可以在本页上定义这些关联，以便在 Port Access（端口访问）页上对服务器执行通电、断电和重新通电操作。

为了使用此功能，你需要：

- Raritan 远程电源条
- 电源 CIM (D2CIM-PWR)

▶ 创建电源关联（使电源条接口与 KVM 目标服务器关联）：

注意：如果电源条与目标服务器（端口）关联，即使你给电源接口指定了另一个名称，也用目标服务器名称取代电源接口名称。

---

1. 在 Power Strip Name（电源条名称）下拉列表上选择电源条。
2. 在 Power Strip Name（电源条名称）下拉列表上选择电源条接口。
3. 对于所有期望的电源关联，重复第一步和第二步。
4. 单击 OK（确定）按钮。显示一条确认消息。

▶ 更改端口名称：

1. 在 Name（名称）字段里输入说明性名称。例如可以使用目标服务器的名称。名称最长为 32 个字母数字字符，可以包含特殊字符。
2. 单击 OK（确定）按钮。

删除电源关联

在把目标服务器和/或电源条与 KXII 断开时，首先应该删除所有电源关联。如果在目标服务器与电源条关联的情况下把目标服务器与 KX II 断开，电源关联仍然存在。在这种情况下，在 Device Settings（设置设置）页上不能访问被断开的目标服务器对应的 Port Configuration（端口配置）页，所以不能正常删除电源关联。

▶ 删除电源条关联：

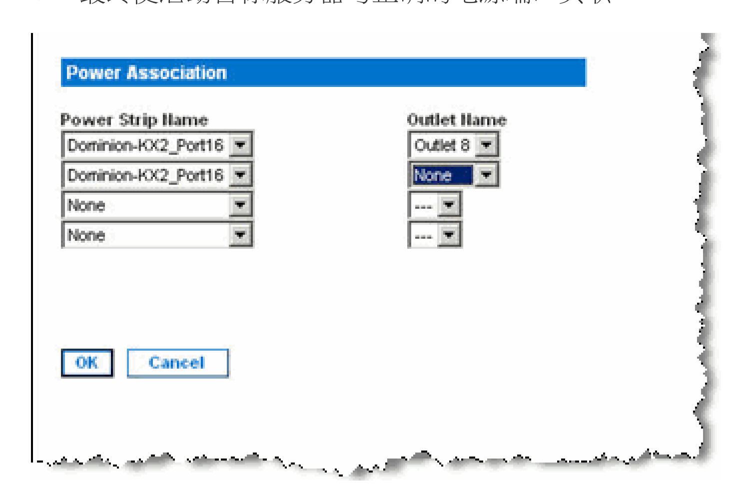
1. 在 Power Strip Name（电源条名称）下拉列表上选择相应的电源条。
2. 在 Outlet Name（电源接口名称）下拉列表上选择相应的电源条接口。
3. 在 Outlet Name（电源接口名称）下拉列表上选择 None（无）。



4. 单击 OK（确定）按钮。电源条/电源接口关联被删除，显示一条确认消息。

▶ 在电源条与目标服务器断开的情况下删除电源条关联：

1. 单击 Device Settings（设备设置）> Port Configuration（端口配置），然后单击活动目标服务器。
2. 使活动目标服务器与被断开的电源端口关联。这将删除被断开的目标服务器的电源关联。
3. 最终使活动目标服务器与正确的电源端口关联。





配置刀片服务器机箱

除了标准服务器和电源条，Dominion KX II 还允许你控制与 Dominion KX II 端口相连的刀片服务器机箱。每次通过 Dominion KX II 最多可以管理八个刀片服务器机箱。

对于标准服务器，在连接刀片服务器机箱之后，Dominion KX II 自动检测它们。当 Dominion KX II 检测到一个刀片服务器机箱时，给它指定一个默认名称，Port Access（端口访问）页显示该刀片服务器机箱、标准目标服务器和电源条（参看***端口访问页*** (p. 41)）。Port Access（端口访问）页采用可展开的分层形式显示刀片服务器机箱，刀片服务器机箱位于分层结构的根部，根下面显示各个有标号的刀片服务器。单击根机箱旁边的展开箭头图标显示各个刀片服务器。

注意：如要按分层顺序查看刀片服务器机箱，必须给刀片服务器机箱配置刀片服务器机箱子类型。

除了 HP® 刀片服务器机箱，在 Port（端口）页上可以配置通用刀片服务器机箱、IBM® 刀片服务器机箱和 Dell® 刀片服务器机箱。必须给与刀片服务器机箱相连的端口配置刀片服务器机箱型号。可以给刀片服务器配置的具体信息，取决于你使用的刀片服务器品牌。如要具体了解每种支持的刀片服务器机箱，参看本节中相应的主题。

支持下列刀片服务器机箱：

- IBM BladeCenter® E 型和 H 型
- Dell PowerEdge® 1855、1955 和 M1000e

Generic（通用）选项允许你配置上述列表没有列出的刀片服务器机箱。从 Dominion KX II 到每个刀片服务器的每个连接均支持 HP BladeSystem c3000 和 c7000。用 Port Group Management（端口组）功能将端口组合成一个机箱。

注意：Dell PowerEdge 1855/1955 刀片服务器还允许你让每个刀片服务器连接一个 Dominion KX II 端口。在采用这种方法连接时，还可以将它们组合在一起创建刀片服务器组。

刀片服务器机箱有两种工作模式：人工配置和自动发现，视刀片服务器机箱的功能而定。如果刀片服务器机箱配置了自动发现，Dominion KX II 跟踪并更新下列各项：

- 何时在机箱上增加一个新刀片服务器。
- 何时从机箱上删除现有刀片服务器。

注意：在使用 IBM BladeCenter E 型和 H 型的情况下，Dominion KX II 只自动发现作为主管理模块的 AMM[1]。

Dominion KX II 还支持用热键将 KVM 访问切换到刀片服务器机箱。对于那些支持用户选择热键的刀片服务器机箱，Port Configuration（端口配置）页将显示这些热键选项。对于有预定义热键的刀片服务器机箱，在选择刀片服务器机箱之后，Port Configuration（端口配置）页自动填充这些热键。例如将 KVM 访问切换到 IBM BladeCenter H 的默认热键是 NumLock+NumLock+SlotNumber，所以在配置过程中选择 IBM BladeCenter H 时，默认应用此热键。参看刀片服务器文档，详细了解热键。

如果有可用的刀片服务器机箱网络浏览器接口，可以配置至刀片服务器机箱网络浏览器接口的连接。在机箱一级，最多可以定义四个连接。第一个连接保留用于连接刀片服务器机箱管理模块 GUI，例如技术支持人员可以用此连接迅速确定机箱配置。

刀片服务器机箱可以用 Dominion KX II Virtual KVM Client (VKC)、Raritan Multi-Platform Client (MPC) 和 CC-SG 管理。通过 VKC 和 MPC 管理刀片服务器的方法与管理标准目标服务器的方法相同。参看***如何使用目标服务器*** (p. 36)和 **CC-SG 管理员指南**了解详情。在 Dominion KX II 上对刀片服务器机箱所作的任何更改，均被传递到这些客户机应用程序。

重要说明：在断开与 Dominion KX II 相连的刀片服务器机箱 CIM 的电源，或者将它与 Dominion KX II 断开时，将关闭此前建立的至该刀片服务器机箱的所有连接。在重新连接 CIM 或给它通电时，必须重新建立连接。

如果将刀片服务器机箱从一个 KX II 端口移到另一个 KX II 端口，在 CC-SG 上给该刀片服务器机箱节点添加的接口将丢失。其他所有信息将被保留。

通用刀片服务器机箱配置

Generic Blade Chassis（通用刀片服务器机箱）选择只提供人工配置操作模式。参看***支持的刀片服务器机箱型号*** (p. 177)、***支持的刀片服务器机箱 CIM*** (参看 "***刀片服务器机箱支持的 CIM***" p. 177) 和***要求和建议的刀片服务器机箱配置*** (p. 180)，了解在配置刀片服务器机箱时所需的其他重要信息。

1. 将刀片服务器连接到 Dominion KX II。参看***第三步：连接设备*** (p. 26) 了解详情。
2. 单击 Device Settings（设备设置）> Port Configuration（端口配置），打开 Port Configuration（端口配置）页。
3. 在 Port Configuration（端口配置）页上单击要配置的刀片服务器机箱的名称。打开 Port（端口）页。
4. 选择 Blade Chassis（刀片服务器机箱）单选按钮。本页显示配置刀片服务器机箱所需的字段。



5. 在 Blade Server Chassis Model（刀片服务器机箱型号）下拉列表上选择 Generic（通用）。
6. 适当配置刀片服务器机箱。
    a. Switch Hot Key Sequence（切换热键）— 定义从 KVM 切换到刀片服务器机箱所用的热键。Switch Hot Key Sequence（切换热键）必须匹配刀片服务器机箱上的 KVM 模块使用的热键。
    b. Administrative Module Primary IP Address/Host Name（管理模块主 IP 地址/主机名）— 不适用。
    c. Maximum Number of Slots（最大插槽数）— 输入刀片服务器机箱可用的默认最大插槽数。
    d. Port Number（端口号）— 刀片服务器机箱默认端口号是 22。 不适用。
    e. Username（用户名）— 不适用。
    f. Password（密码）— 不适用。
7. 必要时更改刀片服务器机箱名称。
8. 选择已安装刀片服务器的每个插槽旁边的 Installed（已安装）复选框，说明已安装在刀片服务器机箱上的刀片服务器。也可以选择 Select All（全选）复选框。必要时更改刀片服务器名称。
9. 可以在本页的 Blade Chassis Managed Links（刀片服务器机箱管理链接）部分配置至可用刀片服务器机箱网络浏览器接口的连接。单击 Blade Chassis Managed Links（刀片服务器机箱管理链接）图标 ► Blade Chassis Managed Links 展开本页的这个部分。

    第一个 URL 链接用于连接刀片服务器机箱管理模块 GUI。

    注意：对在本页这部分输入的 URL 链接的访问，受刀片服务器机箱端口权限的控制。

    ---

    a. Active（活动）— 如在配置此链接之后要激活它，选择 Active（活动）复选框。如不选择此复选框，链接保持闲置状态。即使不选择 Active（活动），仍然可以在链接字段里输入并保存信息。一旦选择 Active（活动），就必须填写 URL 字段。用户名字段和密码字段是可选的，取决于是否需要单点登录。
    b. URL — 输入接口 URL。 要求
    c. Username（用户名）— 输入访问接口所用的用户名。 可选
    d. Password（密码）— 输入访问接口所用的密码。 可选

    注意：对于 DRAC、ILO 和 RSA Web 应用程序，不填写用户名和密码字段，否则连接失败。



e. Username（用户名）字段和 Password（密码）字段都是可选的，包含要与用户名输入和密码输入关联的标签。应该在这些字段里输入用户名字段和密码字段的字段名称，在 Web 应用程序登录屏幕上要使用此用户名和密码。可以查看登录屏幕的 HTML 源代码找到字段*名称*，而非字段标签。参看***添加网络浏览器界面注意事项*** (p. 173)，了解如何添加 Web 浏览器界面。 可选

10. USB 配置文件信息不应用于通用配置。
11. 如果在目标监视器使用此分辨率时显示有问题，在 Target Settings（目标设置）部分选择 720x400 Compensation（720x400 补偿）。
12. 如果用 DCIM-PS2 连接目标，且需要使用扫描代码集 3 和国际键盘，选择 Use international keyboard for scan code set 3（把国际键盘用于扫描代码集 3）。
13. 单击 OK（确定）按钮保存配置。

Dell 刀片服务器机箱配置

参看***支持的刀片服务器机箱型号*** (p. 177)、***支持的刀片服务器机箱 CIM*** (参看 "***刀片服务器机箱支持的 CIM***" p. 177) 和***要求和建议的刀片服务器机箱配置*** (p. 180)，了解在配置刀片服务器机箱时所需的其他重要信息。参看 ***Dell 机箱电缆长度和视频分辨率*** (p. 291)，了解在与 Dominion KX II 一起使用 Dell 机箱时的电缆长度和视频分辨率。

1. 将刀片服务器连接到 Dominion KX II。参看***第三步：连接设备*** (p. 26) 了解详情。
2. 单击 Device Settings（设备设置）> Port Configuration（端口配置），打开 Port Configuration（端口配置）页。
3. 在 Port Configuration（端口配置）页上单击要配置的刀片服务器机箱的名称。打开 Port（端口）页。
4. 选择 Blade Chassis（刀片服务器机箱）单选按钮。本页显示配置刀片服务器机箱所需的字段。
5. 在 Blade Server Chassis Model（刀片服务器机箱型号）下拉列表上选择 Dell 刀片服务器机箱型号。

► 配置 Dell PowerEdge M1000e：

1. 如果选择了 Dell PowerEdge® M1000e，可以使用自动发现。适当配置刀片服务器机箱。在配置可自动发现的刀片服务器机箱之前，必须先配置它允许通过指定端口号进行 SSH 通信（参看***设备服务*** (p. 135)）。此外，此前必须在刀片服务器机箱上创建了一个用户帐号，该用户帐号有相应的验证证书。



a. Switch Hot Key Sequence（切换热键）— 选择从 KVM 切换到刀片服务器所用的热键。 Switch Hot Key Sequence（切换热键）必须匹配刀片服务器机箱上的 KVM 模块使用的热键。

b. Maximum Number of Slots（最大插槽数）— 自动输入刀片服务器机箱可用的默认最大插槽数。

c. Administrative Module Primary IP Address/Host Name（管理模块主 IP 地址/主机名）— 输入刀片服务器机箱的主 IP 地址。 **自动发现模式需要此设置**

d. Port Number（端口号）— 刀片服务器机箱默认端口号是 22。必要时更改端口号。 **自动发现模式需要此设置**

e. Username（用户名）— 输入访问刀片服务器机箱所用的用户名。 **自动发现模式需要此设置**

f. Password（密码）— 输入访问刀片服务器机箱所用的密码。 **自动发现模式需要此设置**

2. 如果希望 Dominion KX II 自动发现机箱上的刀片服务器，选择 Blade Auto-Discovery（刀片服务器自动发现）复选框，单击 Discover Blades on Chassis Now（现在发现机箱上的刀片服务器）按钮。本页显示发现的刀片服务器。

3. 必要时更改刀片服务器机箱名称。如果机箱已经命名了，此字段自动填充机箱名称。如果机箱尚未命名，Dominion KX II 给机箱指定一个名称。Dominion KX II 的默认刀片服务器机箱命名常规是 # Blade_Chassis_Port#。

4. 如果在 Manual（人工）模式下操作，选择已安装刀片服务器的每个插槽旁边的 Installed（已安装）复选框，说明已安装在刀片服务器机箱上的刀片服务器。也可以选择 Select All（全选）复选框。必要时更改刀片服务器名称。

   如果在 Auto-discovery（自动发现）模式下操作，Installed（已安装）字段在发现过程中显示安装了刀片服务器的插槽。

5. 可以在本页的 Blade Chassis Managed Links（刀片服务器机箱管理链接）部分配置至可用刀片服务器机箱网络浏览器接口的连接。单击 Blade Chassis Managed Links（刀片服务器机箱管理链接）图标 ► Blade Chassis Managed Links 展开本页的这个部分。

   第一个 URL 链接用于连接刀片服务器机箱管理模块 GUI。

注意：对在本页这部分输入的 URL 链接的访问，受刀片服务器机箱端口权限的控制。



a. Active（活动）— 如在配置此链接之后要激活它，选择 Active（活动）复选框。如不选择此复选框，链接保持闲置状态。即使不选择 Active（活动），仍然可以在链接字段里输入并保存信息。一旦选择 Active（活动），就必须填写 URL 字段。用户名字段和密码字段是可选的，取决于是否需要单点登录。

b. URL — 输入接口 URL。 参看*刀片服务器机箱* ***URL*** *格式示例* (p. 181)，了解 Dell M1000e 配置示例。

c. Username（用户名）— 输入访问接口所用的用户名。

d. Password（密码）— 输入访问接口所用的密码。

注意：对于 DRAC、ILO 和 RSA Web 应用程序，不填写用户名和密码字段，否则连接失败。

---

e. Username（用户名）字段和 Password（密码）字段都是可选的，包含要与用户名输入和密码输入关联的标签。应该在这些字段里输入用户名字段和密码字段的字段名称，在 Web 应用程序登录屏幕上要使用此用户名和密码。可以查看登录屏幕的 HTML 源代码找到字段*名称*，而非字段标签。参看***添加网络浏览器界面注意事项*** (p. 173)，了解如何添加 Web 浏览器界面。

6. USB 配置文件不应用于 Dell 机箱。

7. 如果在目标监视器使用此分辨率时显示有问题，在 Target Settings（目标设置）部分选择 720x400 Compensation（720x400 补偿）。

8. 如果用 DCIM-PS2 连接目标，且需要使用扫描代码集 3 和国际键盘，选择 Use international keyboard for scan code set 3（把国际键盘用于扫描代码集 3）。

9. 单击 OK（确定）按钮保存配置。

配置 Dell PowerEdge 1855/1955：

1. 如果选择了 Dell PowerEdge 1855/1955，*不能使用*自动发现。适当配置刀片服务器机箱。

   a. Switch Hot Key Sequence（切换热键）— 选择从 KVM 切换到刀片服务器所用的热键。

   b. Maximum Number of Slots（最大插槽数）— 自动输入刀片服务器机箱可用的默认最大插槽数。

   c. Administrative Module Primary IP Address/Host Name（管理模块主 IP 地址/主机名）— 不适用。

   d. Port Number（端口号）— 刀片服务器机箱默认端口号是 22。 不适用。

   e. Username（用户名）— 不适用。



f. Password（密码）— 不适用。

2. 必要时更改刀片服务器机箱名称。
3. 选择已安装刀片服务器的每个插槽旁边的 Installed（已安装）复选框，说明已安装在刀片服务器机箱上的刀片服务器。也可以选择 Select All（全选）复选框。必要时更改刀片服务器名称。
4. 可以在本页的 Blade Chassis Managed Links（刀片服务器机箱管理链接）部分配置至可用刀片服务器机箱网络浏览器接口的连接。单击 Blade Chassis Managed Links（刀片服务器机箱管理链接）图标 ► Blade Chassis Managed Links 展开本页的这个部分。

   第一个 URL 链接用于连接刀片服务器机箱管理模块 GUI。

   注意：对在本页这部分输入的 URL 链接的访问，受刀片服务器机箱端口权限的控制。

   ---

   a. Active（活动）— 如在配置此链接之后要激活它，选择 Active（活动）复选框。如不选择此复选框，链接保持闲置状态。即使不选择 Active（活动），仍然可以在链接字段里输入并保存信息。一旦选择 Active（活动），就必须填写 URL 字段。用户名字段和密码字段是可选的，取决于是否需要单点登录。
   b. URL — 输入接口 URL。 参看***刀片服务器机箱 URL 格式示例*** (p. 181)，了解 Dell PowerEdge 1855/1955 配置示例。
   c. Username（用户名）— 输入访问接口所用的用户名。
   d. Password（密码）— 输入访问接口所用的密码。

   注意：对于 DRAC、ILO 和 RSA Web 应用程序，不填写用户名和密码字段，否则连接失败。

   ---

   e. Username（用户名）字段和 Password（密码）字段都是可选的，包含要与用户名输入和密码输入关联的标签。应该在这些字段里输入用户名字段和密码字段的字段名称，在 Web 应用程序登录屏幕上要使用此用户名和密码。可以查看登录屏幕的 HTML 源代码找到字段*名称*，而非字段标签。参看***添加网络浏览器界面注意事项*** (p. 173)，了解如何添加 Web 浏览器界面。
5. USB 配置文件不应用于 Dell 机箱。
6. 单击 OK（确定）按钮保存配置。



IBM 刀片服务器机箱配置

参看***支持的刀片服务器机箱型号*** (p. 177)、***支持的刀片服务器机箱 CIM*** (参看 "***刀片服务器机箱支持的 CIM***" p. 177) 和***要求和建议的刀片服务器机箱配置*** (p. 180)，了解在配置刀片服务器机箱时所需的其他重要信息。

1. 将刀片服务器连接到 Dominion KX II。参看***第三步：连接设备*** (p. 26) 了解详情。
2. 单击 Device Settings（设备设置）> Port Configuration（端口配置），打开 Port Configuration（端口配置）页。
3. 在 Port Configuration（端口配置）页上单击要配置的刀片服务器机箱的名称。打开 Port（端口）页。
4. 选择 Blade Chassis（刀片服务器机箱）单选按钮。本页显示配置刀片服务器机箱所需的字段。
5. 在 Blade Server Chassis Model（刀片服务器机箱型号）下拉列表上选择 IBM® 刀片服务器机箱型号。

▶ **配置 IBM BladeCenter H 和 E：**

1. 如果选择了 IBM BladeCenter® H 或 E，可以使用自动发现。适当配置刀片服务器机箱。在配置可自动发现的刀片服务器机箱之前，必须先配置它允许通过指定端口号进行 SSH 通信（参看***设备服务*** (p. 135)）。此外，此前必须在刀片服务器机箱上创建了一个用户帐号，该用户帐号有相应的验证证书。 Dominion KX II 只支持 AMM[1] 自动发现。
   a. Switch Hot Key Sequence（切换热键）— 预定义。
   b. Maximum Number of Slots（最大插槽数）— 自动输入刀片服务器机箱可用的默认最大插槽数。
   c. Administrative Module Primary IP Address/Host Name（管理模块主 IP 地址/主机名）— 输入刀片服务器机箱的主 IP 地址。 **自动发现模式需要此设置**
   d. Port Number（端口号）— 刀片服务器机箱默认端口号是 22。必要时更改端口号。 **自动发现模式需要此设置**
   e. Username（用户名）— 输入访问刀片服务器机箱所用的用户名。**自动发现模式需要此设置**
   f. Password（密码）— 输入访问刀片服务器机箱所用的密码。 **自动发现模式需要此设置**
2. 如果希望 Dominion KX II 自动发现机箱上的刀片服务器，选择 Blade Auto-Discovery（刀片服务器自动发现）复选框，单击 Discover Blades on Chassis Now（现在发现机箱上的刀片服务器）按钮。本页显示发现的刀片服务器。



3. 必要时更改刀片服务器机箱名称。如果机箱已经命名了，此字段自动填充机箱名称。如果机箱尚未命名，Dominion KX II 给机箱指定一个名称。Dominion KX II 的默认刀片服务器机箱命名常规是 #Blade_Chassis_Port#。

4. 如果在 Manual（人工）模式下操作，选择已安装刀片服务器的每个插槽旁边的 Installed（已安装）复选框，说明已安装在刀片服务器机箱上的刀片服务器。也可以选择 Select All（全选）复选框。必要时更改刀片服务器名称。

   如果在 Auto-discovery（自动发现）模式下操作，Installed（已安装）字段在发现过程中显示安装了刀片服务器的插槽。

5. 可以在本页的 Blade Chassis Managed Links（刀片服务器机箱管理链接）部分配置至可用刀片服务器机箱网络浏览器接口的连接。单击 Blade Chassis Managed Links（刀片服务器机箱管理链接）图标 ► Blade Chassis Managed Links 展开本页的这个部分。

   第一个 URL 链接用于连接刀片服务器机箱管理模块 GUI。

   注意：对在本页这部分输入的 URL 链接的访问，受刀片服务器机箱端口权限的控制。

   a. Active（活动）— 如在配置此链接之后要激活它，选择 Active（活动）复选框。如不选择此复选框，链接保持闲置状态。即使不选择 Active（活动），仍然可以在链接字段里输入并保存信息。一旦选择 Active（活动），就必须填写 URL 字段。用户名字段和密码字段是可选的，取决于是否需要单点登录。

   b. URL — 输入接口 URL。 参看***刀片服务器机箱 URL 格式示例*** (p. 181)，了解 IBM BladeCenter 配置示例。

   c. Username（用户名）— 输入访问接口所用的用户名。

   d. Password（密码）— 输入访问接口所用的密码。

   注意：对于 DRAC、ILO 和 RSA Web 应用程序，不填写用户名和密码字段，否则连接失败。

   e. Username（用户名）字段和 Password（密码）字段都是可选的，包含要与用户名输入和密码输入关联的标签。应该在这些字段里输入用户名字段和密码字段的字段名称，在 Web 应用程序登录屏幕上要使用此用户名和密码。可以查看登录屏幕的 HTML 源代码找到字段*名称*，而非字段标签。参看***添加网络浏览器界面注意事项*** (p. 173)，了解如何添加 Web 浏览器界面。



6. 必要时给刀片服务器机箱定义 USB 配置文件，或者选择现有的 USB 配置文件。单击 USB Profiles（USB 配置文件）-> Select USB Profiles for Port（给端口选择 USB 配置文件）图标 ► Select USB Profiles for Port 或 Apply（应用）-> Select Profiles to Other Ports（给其他端口选择配置文件）图标 ► Apply Selected Profiles to Other Ports，展开本页的这些部分。参看*配置 USB 配置文件（端口页）* (p. 182)。
7. 单击 OK（确定）按钮保存配置。

► 配置 IBM BladeCenter（其他）：

1. 如果选择了 IBM BladeCenter（其他），*不能使用*自动发现。适当配置刀片服务器机箱。
   a. Switch Hot Key Sequence（切换热键）— 选择从 KVM 切换到刀片服务器所用的热键。
   b. Administrative Module Primary IP Address/Host Name（管理模块主 IP 地址/主机名）— 输入刀片服务器机箱的主 IP 地址。不适用。
   c. Maximum Number of Slots（最大插槽数）— 输入刀片服务器机箱可用的默认最大插槽数。
   d. Port Number（端口号）— 刀片服务器机箱默认端口号是 22。 不适用。
   e. Username（用户名）— 不适用。
   f. Password（密码）— 不适用。
2. 必要时更改刀片服务器机箱名称。
3. 选择已安装刀片服务器的每个插槽旁边的 Installed（已安装）复选框，说明已安装在刀片服务器机箱上的刀片服务器。也可以选择 Select All（全选）复选框。必要时更改刀片服务器名称。如果刀片服务器尚未命名，Dominion KX II 给刀片服务器指定一个名称。默认刀片服务器命名常规是 # Blade_Chassis_Port#_Slot#。
4. 可以在本页的 Blade Chassis Managed Links（刀片服务器机箱管理链接）部分配置至可用刀片服务器机箱网络浏览器接口的连接。单击 Blade Chassis Managed Links（刀片服务器机箱管理链接）图标 ► Blade Chassis Managed Links 展开本页的这个部分。

   第一个 URL 链接用于连接刀片服务器机箱管理模块 GUI。

   注意：对在本页这部分输入的 URL 链接的访问，受刀片服务器机箱端口权限的控制。



a. Active（活动）— 如在配置此链接之后要激活它，选择 Active（活动）复选框。如不选择此复选框，链接保持闲置状态。即使不选择 Active（活动），仍然可以在链接字段里输入并保存信息。一旦选择 Active（活动），就必须填写 URL 字段。用户名字段和密码字段是可选的，取决于是否需要单点登录。

b. URL — 输入接口 URL。 参看***刀片服务器机箱 URL 格式示例*** (p. 181)，了解 IBM BladeCenter 配置示例。

c. Username（用户名）— 输入访问接口所用的用户名。

d. Password（密码）— 输入访问接口所用的密码。

注意：对于 DRAC、ILO 和 RSA Web 应用程序，不填写用户名和密码字段，否则连接失败。

---

e. Username（用户名）字段和 Password（密码）字段都是可选的，包含要与用户名输入和密码输入关联的标签。应该在这些字段里输入用户名字段和密码字段的字段名称，在 Web 应用程序登录屏幕上要使用此用户名和密码。可以查看登录屏幕的 HTML 源代码找到字段*名称*，而非字段标签。参看***添加网络浏览器界面注意事项*** (p. 173)，了解如何添加 Web 浏览器界面。

5. IBM（其他）配置不使用 USB 配置文件。
6. 如果在目标监视器使用此分辨率时显示有问题，在 Target Settings（目标设置）部分选择 720x400 Compensation（720x400 补偿）。
7. 如果用 DCIM-PS2 连接目标，且需要使用扫描代码集 3 和国际键盘，选择 Use international keyboard for scan code set 3（把国际键盘用于扫描代码集 3）。
8. 单击 OK（确定）按钮保存配置。

添加网络浏览器界面注意事项

可以添加一个网络浏览器界面，建立至使用嵌入 Web 服务器的设备的连接。也可以用网络浏览器界面连接任何 Web 应用程序，例如与 RSA、DRAC 或 ILO Processor 卡关联的 Web 应用程序。

必须配置 DNS，否则不解析 URL。如果输入 IP 地址，不必配置 DNS。

▶ 添加网络浏览器界面：

1. 输入 Web Browser Interface（网络浏览器界面）的默认名称。必要时更改 Name（名称）字段里的名称。
2. 在 URL 字段里输入 Web 应用程序的 URL 或域名。必须输入 Web 应用程序要读取的用户名和密码所在的 URL。

   使用下列正确格式：

- http(s)://192.168.1.1/login.asp
- http(s)://www.example.com/cgi/login
- http(s)://example.com/home.html

3. 输入访问此界面所需的用户名和密码。**可选**
4. 如果输入用户名和密码，在 Username（用户名）字段和 Password（密码）字段里输入 Web 应用程序登录屏幕所用的用户名字段和密码字段的字段名称。必须查看登录屏幕的 HTML 源代码找到字段名称，而非字段标签。

查找字段名称注意事项：

- 在 Web 应用程序登录页面的 HTML 源代码里搜索字段标签，例如 Username 和 Password。
- 在找到字段标签之后，查看标记旁边类似下面这样的代码：name="user"。引号里面的单词就是字段名。



HP 刀片服务器机箱配置（端口组管理）

Dominion KX II 可以将与某些类型的刀片服务器相连的端口组合成一个组，表示刀片服务器机箱。尤其是在从每个刀片服务器将 Dell® PowerEdge® 1855/1955 连接到一个 Dominion KX II 端口时，将 HP® BladeServer 刀片服务器和 Dell® PowerEdge® 1855/1955 刀片服务器组合在一起。

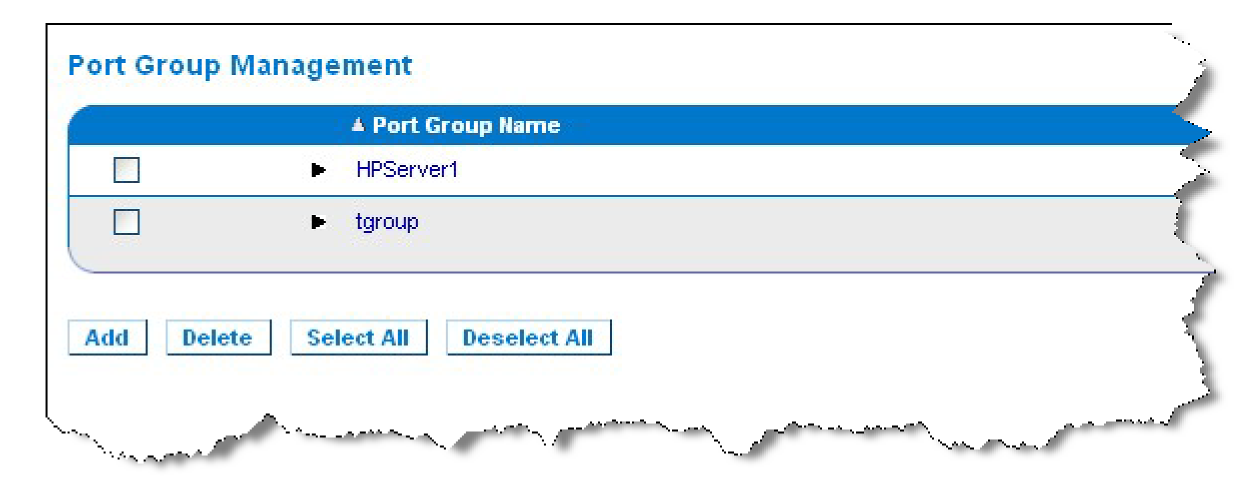
在 Port Group Management（端口组管理）页上，机箱用 Port Group Name（端口组名称）标识，组定义为 Blade Server Group（刀片服务器组）。Port Group（端口组）只包括作为标准 KVM 端口配置的端口，不包括作为刀片服务器机箱配置的端口。一个端口只能是一个组的成员。

与刀片服务器机箱上的集成 KVM 模块相连的端口配置为刀片服务器机箱子类型。这些端口可以包括在端口组里。

如果 Dominion KX II 端口连接刀片服务器机箱上的集成 KVM 模块，但不连接各个刀片服务器，这些端口配置为刀片服务器机机箱类型。这些端口不能包括在端口组里，Select Port for Group（给组选择端口）和 Available（可用）列表不显示它们。

如果将一个标准 KVM 端口包括在端口组里，然后将它重新配置为刀片服务器机机箱类型，必须先将它从端口组里删除掉。

Port Groups（端口组）用 Backup and Restore（备份和恢复）选项恢复（参看***备份和恢复*** (p. 206)）。



► 添加端口组：

1. 单击 Device Settings（设备设置）> Port Group Management（端口组管理），打开 Port Group Management（端口组管理）页。
2. 单击 Add（添加）按钮，打开 Port Group（端口组）页。
3. 输入 Port Group Name（端口组名称）。端口组名称不区分大小写，最多 32 个字符。

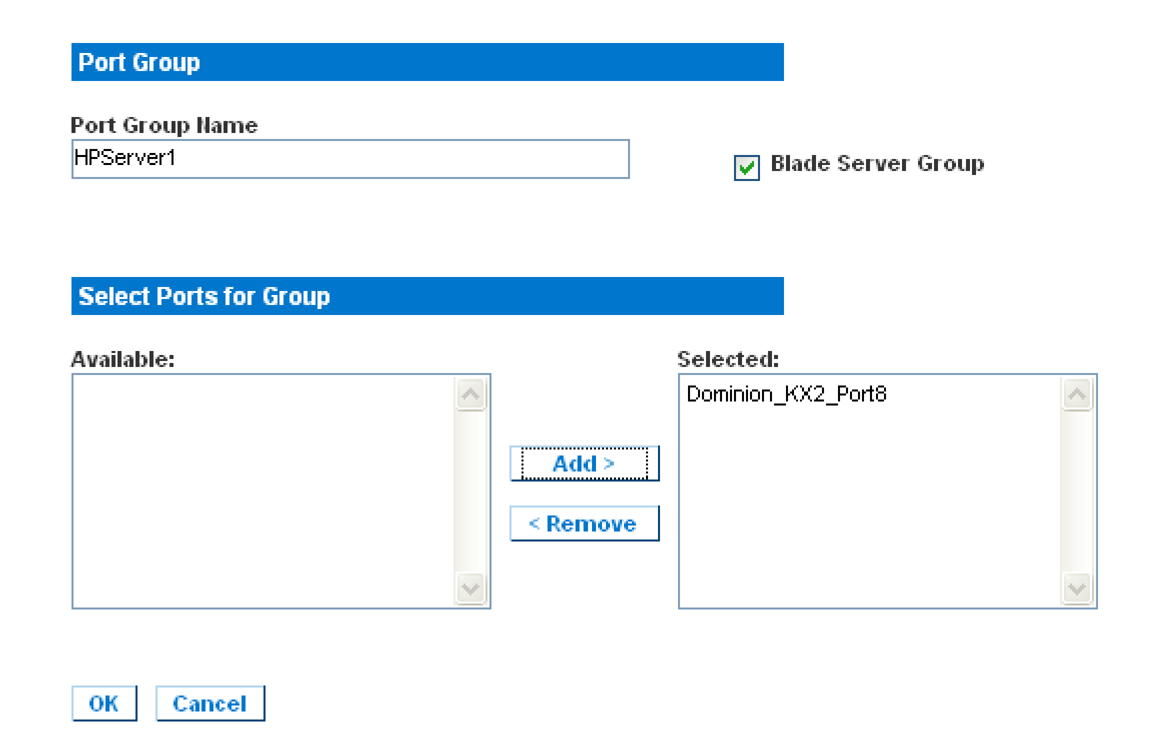
4. 选择 Blade Server Group（刀片服务器组）复选框。

   如果要指定将这些端口连接到刀片服务器机箱（例如 HP c3000 或 Dell PowerEdge 1855）上的刀片服务器，选择 Blade Server Group（刀片服务器组）复选框。

   注意：这对那些希望根据机箱组织管理 HP 刀片服务器的 CC-SG 用户来说尤其重要，虽然每个刀片服务器连接一个 Dominion KX II 端口。

   ---

5. 在 Select Ports for Group（给组选择端口）部分，单击 Available（可用）字段里的一个端口。单击 Add（添加）按钮将该端口添加到组。该端口被移动到 Selected（已选择）字段。
6. 单击 OK（确定）按钮添加端口组。



▶ **编辑端口组信息：**

1. 在 Port Group Management（端口组管理）页上单击要编辑的端口组的链接。打开 Port Group（端口组）页。
2. 根据需要编辑信息。
3. 单击 OK（确定）按钮保存更改。



▶ **删除端口组：**

1. 在 Port Group Management（端口组管理）页上单击要删除的端口组对应的复选框。
2. 单击 Delete（删除）按钮。
3. 单击确认消息上的 OK（确定）按钮。

支持的刀片服务器机箱型号

下表列出 Dominion KX II 支持的刀片服务器机箱型号，以及在 Dominion KX II 应用中配置机箱型号时应给它们选择的相应配置文件。如果选择了 Blade Chassis（刀片服务器机箱）单选按钮，显示 Blade Server Chassis Model（刀片服务器机箱型号）下拉列表，可以在 Port Configuration（端口配置）页上选择这些型号的列表。如要详细了解如何配置每种刀片服务器机箱，参看本节中相应的主题。

刀片服务器机箱型号	**Dominion KX II 配置文件**
Dell® PowerEdge® 1855/1955	Dell PowerEdge 1855/1955
Dell PowerEdge M1000e	Dell PowerEdge M1000e
IBM® BladeCenter® S	IBM（其他）
IBM BladeCenter H	IBM BladeCenter H
IBM BladeCenter T	IBM（其他）
IBM BladeCenter HT	IBM（其他）
IBM BladeCenter E	IBM BladeCenter E
HP®	用端口组管理功能配置。参看 ***HP 刀片服务器机箱配置（端口组管理）*** (p. 175)。

刀片服务器机箱支持的 CIM

通过 Dominion KX II 管理的刀片服务器机箱支持下列 CIM：

- DCIM-PS2
- DCIM-USBG2
- D2CIM-VUSB
- D2CIM-DVUSB

下表列出 Dominion KX II 支持的每种刀片服务器机箱型号支持的 CIM。



刀片服务器机箱	连接方法	推荐的 CIM
Generic	如果在连接被配置为 Generic 的刀片服务器机箱时使用 D2CIM-VUSB 或 D2CIM-DVUSB，可以在 Port Configuration（端口配置）页和客户机的 USB Profile（USB 配置文件）菜单上选择 USB 配置文件。但通用刀片服务器机箱不支持虚拟媒体，客户机禁用 Virtual Media（虚拟媒体）菜单。	• DCIM-PS2 • DCIM-USBG 2
Dell® PowerEdge® 1855	包括下列三个 KVM 模块之一： • 模拟 KVM Ethernet 切换模块（标准） • 数字访问 KVM 切换模块（可选） • KVM 切换模块（在 2005 年 4 月之前销售的系统上是标准配置） 这些切换器配有定制连接器，允许将两个 PS/2 设备和一台监视器接到系统上。 资料来源：*Dell PowerEdge 1855 用户指南*	• DCIM-PS2
Dell PowerEdge 1955	可以安装两种 KVM 模块之一： • 模拟 KVM 切换模块 • 数字访问 KVM 切换模块 两个模块都允许你用随系统一并提供的定制电缆，将一个 PS/2 兼容键盘、一个鼠标和一台监视器接到系统上。 资料来源：*Dell PowerEdge 1955 用户手册*	• DCIM-PS2
Dell PowerEdge M1000e	KVM 切换模块 (iKVM) 集成在此机箱上。 iKVM 兼容下列外设： • USB 键盘和 USB 鼠标 • 支持 DDC 的 VGA 监视器 资料来源：*Dell Chassis Management Controller Firmware V1.0 用户指南*	• DCIM-USBG 2
HP® BladeSystem c3000	HP c-Class 刀片服务器 SUV 电缆允许你直接将监视器和 USB 设备接到刀片服务器上，可以执行刀片服务器机箱管理、配置和诊断操作。 资料来源：*HP ProLiant™ BL480c 刀片服务器维护和维修指南*	• DCIM-USBG 2 • D2CIM-VUSB • D2CIM-DVUSB（用于标准 KVM 端口操作，没有 KVM 选项）



刀片服务器机箱	连接方法	推荐的 CIM
HP BladeSystem c7000	HP c-Class 刀片服务器 SUV 电缆允许你直接将监视器和 USB 设备接到刀片服务器上，可以执行刀片服务器管理、配置和诊断操作。 资料来源：*HP ProLiant BL480c 刀片服务器维护和维修指南*	• DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB（用于标准 KVM 端口操作）
IBM® BladeCenter® S	高级管理模块 (Advanced Management Module, AMM) 给所有刀片服务器机箱提供系统管理功能和键盘/视频/鼠标 (KVM) 多路复用。 AMM 连接包括一个串行端口、一个视频连接端口、一个远程管理端口 (Ethernet) 和两个用于连接键盘和鼠标的 USB v2.0 端口。 资料来源：*实现 IBM BladeCenter S 机箱*	• DCIM-USBG2
IBM BladeCenter H	BladeCenter H 机箱标准配置一个高级管理模块。 资料来源：*IBM BladeCenter 产品和技术*	• DCIM-USBG2 • D2CIM-DVUSB
IBM BladeCenter E	最新型 BladeCenter E 机箱 (8677-3Rx) 标准配置一个高级管理模块。 资料来源：*IBM BladeCenter 产品和技术*	• DCIM-USBG2 • D2CIM-DVUSB
IBM BladeCenter T	BladeCenter T 机箱标准配置一个高级管理模块。 与标准 BladeCenter 机箱相比，BladeCenter T 机箱上的 KVM 模块和管理模块是分离部件。管理模块面板上只有 LED 指示灯，显示其状态。所有 Ethernet 和 KVM 连接均通过背板连接 LAN 模块和 KVM 模块。 机箱背面的 KVM 模块是热交换模块，有两个 PS/2 连接器连接键盘和鼠标，有一个系统状态显示板，有一个 HD-15 视频连接器。 资料来源：*IBM BladeCenter 产品和技术*	• DCIM-PS2
IBM BladeCenter HT	BladeCenter HT 机箱标准配置一个高级管理模块。此模块具备机箱管理能力和本地 KVM 功能。 资料来源：*IBM BladeCenter 产品和技术*	• DCIM-USBG2

注意：为了支持自动发现，IBM BladeCenter Model H 和 E 必须使用固件版本为 BPET36K 或更高版本的 AMM。

注意：在使用 IBM BladeCenter E 型和 H 型的情况下，Dominion KX II 只自动发现作为主管理模块的 AMM[1]。

要求和建议的刀片服务器机箱配置

下表说明在配置刀片服务器机箱使用 Dominion KX II 时要考虑的限制和约束。Raritan 建议你采用下列所有信息。

刀片服务器机箱	要求/建议的操作
Dell® PowerEdge® M1000e	• 禁用 iKVM GUI 屏幕保护。如果不这样做，将显示 Authorize（授权）对话框，iKVM 不能正常工作。 • 退出 iKVM GUI 菜单，将 Dell 机箱连接到 Raritan CIM。 • 配置 iKVM GUI 主菜单，按插槽或名称选择目标刀片服务器。如果不这样做，iKVM 可能无法正常工作。 • *切勿*在 iKVM GUI Setup Scan（设置扫描）菜单上给任何插槽指定扫描操作。否则，iKVM 可能无法正常工作。 • *切勿*在 iKVM GUI Setup Broadcast（设置广播）菜单上给任何插槽指定广播键盘/鼠标操作。否则，iKVM 可能无法正常工作。 • 指定一个热键调用 iKVM GUI。此热键还必须在 Dominion KX II 端口配置过程中加以确认。否则在客户机上输入热键时，iKVM 可能会误操作。 • 确保在用 Dell CMC GUI 配置 iKVM 过程中*不*选择 Front Panel USB/Video Enabled（启用面板 USB/视频）。否则，机箱面板上的连接的优先级高于背板上的 Dominion KX II 连接，致使 iKVM 不能正常工作。显示一条消息：由于面板当前处于活动状态，用户被禁用。 • 确保在用 Dell CMC GUI 配置 iKVM 过程中*不*选择 Allow access to CMC CLI from iKVM（允许在 iKVM 上访问 CMC CLI）。 • 如在连接刀片服务器机箱之后不显示 iKVM GUI，将 Screen Delay Time（屏幕延迟时间）设置为 8 秒。 • 建议在 iKVM GUI Flag Setup（标志设置）过程中选择 Timed（定时）和 Displayed（显示）。这样，你可以直观确认至期望的刀片服务器插槽的连接。
Dell PowerEdge 1855/1955	• 禁用 iKVM GUI 屏幕保护。如果不这样做，将显示 Authorize（授权）对话框，iKVM 不能正常工作。 • 退出 iKVM GUI 菜单，将 Dell 机箱连接到 Raritan CIM。 • 配置 iKVM GUI 主菜单，按插槽或名称选择目标刀片服务器。如果不这样做，iKVM 可能无法正常工作。



刀片服务器机箱	要求/建议的操作
	• *切勿在* iKVM GUI Setup Scan（设置扫描）菜单上给任何插槽指定扫描操作，否则 iKVM 可能无法正常工作。 • 如在连接刀片服务器机箱之后不显示 iKVM GUI，将 Screen Delay Time（屏幕延迟时间）设置为 8 秒。 • 建议在 iKVM GUI Flag Setup（标志设置）过程中选择 Timed（定时）和 Displayed（显示）。这样，你可以直观确认至期望的刀片服务器插槽的连接。
IBM®/Dell 自动发现	• 建议你在应用刀片服务器级访问权时，启用自动发现。否则，在刀片服务器机箱上设置访问权。 • 必须在刀片服务器机箱管理模块上启用 Secure Shell (SSH)。 • 在刀片服务器机箱管理模块上配置的 SSH 端口必须匹配在 Port Configuration（端口配置）页上输入的端口号。
IBM KX2 虚拟媒体	• 只有 IBM BladeCenter® H 型和 E 型支持 Raritan Dominion KX II 虚拟媒体。要求使用 D2CIM-DVUSB。黑色 D2CIM-DVUSB 低速 USB 连接器连接设备背板上的高级管理模块 (AMM)。灰色 D2CIM-DVUSB 高速 USB 连接器连接设备面板上的介质托盘 (Media Tray, MT)。要求使用 USB 延长电缆。

注意：所有 IBM BladeCenter 必须使用固件版本为 BPET36K 或更高版本的 AMM，才能与 Dominion KX II 一起工作。

注意：在使用 IBM BladeCenter E 型和 H 型的情况下，Dominion KX II 只自动发现作为主管理模块的 AMM[1]。

刀片服务器机箱 URL 格式示例

下表举例说明在 Dominion KX II 上给刀片服务器机箱配置的 URL 格式。

刀片服务器机箱	URL 格式示例
Dell® M1000e	• URL：https://192.168.60.44/cgi-bin/webcgi/login • Username（用户名）：root • Username Field（用户名字段）：user • 密码：calvin • Password Field（密码字段）：password
Dell 1855	• URL：https://192.168.60.33/Forms/f_login • Username（用户名）：root • Username Field（用户名字段）：TEXT_USER_NAME



刀片服务器机箱	URL 格式示例
	• 密码：calvin • Password Field（密码字段）：TEXT_PASSWORD
IBM® BladeCenter® E 型和 H 型	• http://192.168.84.217/private/welcome.ssi

配置 USB 配置文件（端口页）

在 Port（端口）页的 Select USB Profiles for Port（给端口选择 USB 配置文件）部分给一个端口选择可用的 USB 配置文件。当 VKC 用户通过该端口连接 KVM 目标服务器时，可以使用在 Port（端口）页上选择的 USB 配置文件。默认设置是 Windows 2000® 操作系统配置文件、Windows XP® 操作系统配置文件和 Windows Vista® 操作系统配置文件。参看 ***USB 配置文件*** (p. 98)了解 USB 配置文件。

*注意：为了给端口设置 USB 配置文件，必须将安装了兼容固件的 VM-CIM 连接到安装了最新版固件的 Dominion KX II。参看***升级 CIM** *(p. 210)。*

左边的 Available（可用）列表显示可以给端口指定的配置文件。右边的 Selected（已选择）列表显示给端口选择的配置文件。在任何一个列表上选择一个配置文件时，Profile Description（配置文件说明）字段显示该配置文件的说明和用途。

除了选择一组配置文件使它们可用于一个 KVM 端口，还可以给该端口指定首选配置文件，将这些设置应用于一个端口，而不应用于其他 KVM 端口。

*注意：如果使用 DCIM-VUSB 或 DCIM-DVUSB，参看***在使用 Mac OS-X USB 配置文件和 DCIM-VUSB 时的鼠标模式** *(参看 "***在与 DCIM-VUSB 一起使用 Mac OS-X USB 配置文件时的鼠标模式***" p. 105)，了解如何使用 Mac OS-X® USB 配置文件。*

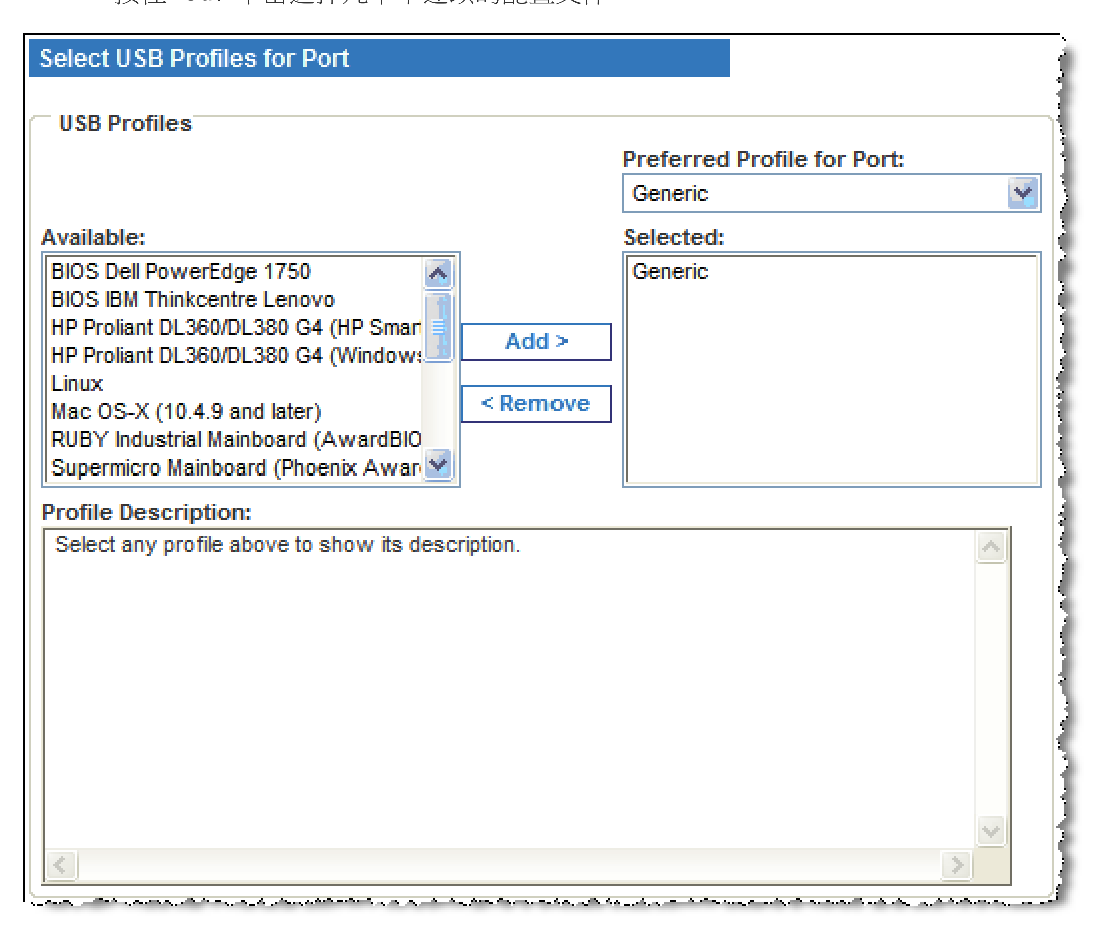
► 打开端口页：

1. 选择 Device Settings（设备设置）> Port Configuration（端口配置）。打开 Port Configuration（端口配置）页。
2. 单击要编辑的 KVM 端口的端口名称。打开 Port（端口）页。



▶ 给 KVM 端口选择 USB 配置文件：

1. 在 Select USB Profiles for Port（给端口选择 USB 配置文件）部分的 Available（可用）列表上选择一个或多个 USB 配置文件。
   - 按住 Shift 单击选择几个连续配置文件。
   - 按住 Ctrl 单击选择几个不连续的配置文件。



2. 单击 Add（添加）按钮。Selected（已选择）列表显示选择的配置文件。这些配置文件可用于与端口相连的 KVM 目标服务器。

▶ 指定首选 USB 配置文件：

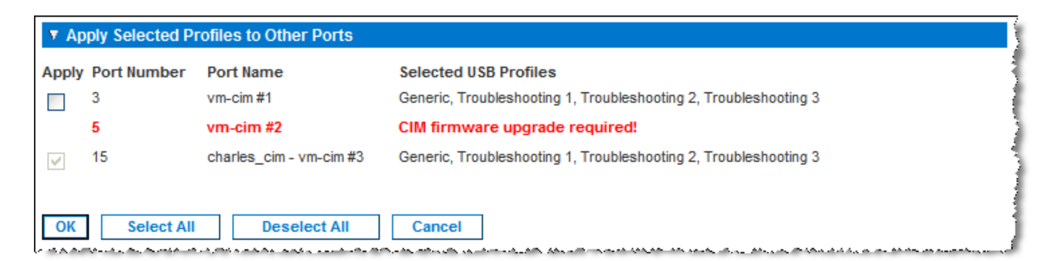
1. 在给一个端口选择多个可用配置文件之后，在 Preferred Profile for Port（首选端口配置文件）菜单上选择一个配置文件。默认值是 Generic。在连接 KVM 目标服务器时，使用所选的配置文件。必要时可以更改为其他任何 USB 配置文件。

▶ 删除选择的 USB 配置文件：

1. 在 Select USB Profiles for Port（给端口选择 USB 配置文件）部分的 Selected（选择）列表上选择一个或多个配置文件。
   - 按住 Shift 单击选择几个连续配置文件。
   - 按住 Ctrl 单击选择几个不连续的配置文件。
2. 单击 Remove（删除）按钮。Available（可用）列表显示选择的配置文件。这些配置文件不再可用于与此端口相连的 KVM 目标服务器。

▶ 将选择的配置文件应用于多个端口：

1. 在 Apply Selected Profiles to Other Ports（将选择的配置文件应用于其他端口）部分选择要应用最新选择的 USB 配置文件的 KVM 端口对应的 Apply（应用）复选框。



   - 如要选择所有 KVM 端口，单击 Select All（全选）。
   - 如要取消所有 KVM 端口，单击 Deselect All（全部取消）。



配置 Dominion KX II 本地端口设置

可以在 Local Port Settings（本地端口设置）页上定制 Dominion KX II Local Console 的许多设置，包括键盘、热键、视频切换延迟、节电模式、本地用户界面分辨率设置和本地用户验证。可以在本地端口上进一步更改 USB 配置文件。

对于 KX2-832 和 KX2-864，还可以在 Local Port Settings（本地端口设置）页上配置扩展本地端口。扩展本地端口可以连接 Paragon 切换器或用户工作站，从而扩大本地端口的范围。可以像配置标准本地端口一样配置键盘、热键、视频切换延迟、节电模式、本地用户界面分辨率设置和本地用户验证设置。可以在 Remote Console 和 Local Console 上配置扩展本地端口。参看 ***KX2-832 和 KX2-864 标准本地端口设置和扩展本地端口设置*** (p. 188)，进一步了解标准本地端口和扩展本地端口。

注意：如果在 KX2-832 和 KX2-864 上启用扩展本地端口，但此端口没有连接任何东西，在通过本地端口切换到目标服务器时有 2-3 秒延迟。

▶ 配置本地端口设置：

注意：在 Local Port Settings（本地端口设置）页上更改某些设置之后，要重新启动正在使用的浏览器。如果在更改设置时重新启动浏览器，将记录设置步骤。

---

1. 选择 Device Settings（设备设置）> Local Port Settings（本地端口设置）。打开 Local Port Settings（本地端口设置）页。
2. 选择 Enable Standard Local Port（启用标准本地端口）旁边的复选框启用它。取消此复选框禁用它。默认启用标准本地端口，但可以按需要禁用它。在进行更改时，重新启动浏览器。如果使用级联功能，将关闭此功能，不能同时使用这两个功能。
3. 如果使用 KX2-832 或 KX2-864 设备，选择 Extended Local Port（扩展本地端口）旁边的复选框启用它。取消此复选框禁用它。如果使用智能卡功能，必须禁用扩展本地端口。在进行更改时，重新启动浏览器。

   如果同时禁用标准本地端口和扩展本地端口，不能访问本地端口。如果尝试通过被禁用的本地端口访问 KX2-832 或 KX2-864，显示一条错误消息，说明设备处于远程管理模式下，登录名被禁用了。

   注意：如果把 KX2-832 和 KX2-864 用做级联设备，必须通过扩展本地端口把它们连接到基础 Dominion KX II。

   注意：如果把 Paragon 设备连接到 KX2-832 或 KX2-864 扩展本地端口，必须用远程客户机更改 USB 配置文件。



4. 如果使用级联功能，选择 Enable Local Port Device Tiering（启用本地端口设备级联）复选框，在 Tier Secret（级联密码）字段里输入级联密码。为了配置级联，还必须在 Device Services（设备服务）页上配置基础设备。参看***配置和启用级联*** (p. 137)详细了解级联。
5. 在键盘类型下拉列表上的选项中选择合适的键盘类型。在进行更改时，重新启动浏览器。
   - US（美国英语）
   - US/International（美国英文/国际）
   - United Kingdom（英国英语）
   - French (France)（法文[法国]）
   - German (Germany)（德文[德国]）
   - JIS（日本工业标准）
   - Simplified Chinese（简体中文）
   - Traditional Chinese（繁体中文）
   - Dubeolsik Hangul（朝鲜文）
   - German (Switzerland)（德文[瑞士]）
   - Portuguese（葡萄牙）
   - Norwegian (Norway)（挪威文[挪威]）
   - Swedish (Sweden)（瑞典文[瑞典]）
   - Danish (Denmark)（丹麦文[丹麦]）
   - Belgian (Belgium)（比利时）

注意：中文键盘、日文键盘和朝鲜文键盘仅用于显示。Dominion KX II Local Console 功能目前不支持本地语言输入。

6. 选择本地端口热键。在显示目标服务器界面时，可以用本地端口热键返回 Dominion KX II Local Console 界面。默认设置是按双击 Scroll Lock，但可以在下拉列表上选择任何组合键：

热键：	执行此操作：
双击 Scroll Lock	迅速按两次 Scroll Lock 键
双击 Num Lock	迅速按两次 Num Lock 键
双击 Caps Lock	迅速按两次 Caps Lock 键
双击左 Alt 键	迅速按两次左 Alt 键
双击左 Shift 键	迅速按两次左 Shift 键



热键：	执行此操作：
双击左 Ctrl 键	迅速按两次左 Ctrl 键

7. 选择 Local Port Connect key（本地端口连接键）。用连接键连接目标服务器，切换到另一台目标服务器。可以用热键断开目标服务器，返回本地端口 GUI。连接键适用于标准服务器和刀片服务器机箱。在创建本地端口连接键之后，GUI 导航面板显示该键，所以你可以用它作为参考。参看***连接键示例*** (p. 242)了解连接键顺序示例。
8. 必要时将 Video Switching Delay（视频切换延迟）设置为 0-5 秒。通常使用 0，除非需要更长的时间（某些监视器要求的视频切换时间较长）。
9. 如果要使用节电功能：
   a. 选择 Power Save Mode（节电模式）复选框。
   b. 设置在启动节电模式之前经过的时间（分钟）。
10. 在 Resolution（分辨率）下拉列表上选择 Dominion KX II Local Console 的分辨率。在进行更改时，重新启动浏览器。
    - 800x600
    - 1024x768
    - 1280x1024
11. 在 Refresh rate（刷新速率）下拉列表上选择刷新速率。 在进行更改时，重新启动浏览器。
    - 60 Hz
    - 75 Hz
12. 选择本地用户验证类型。
    - Local/LDAP/RADIUS。这是建议的选项。参看***远程验证*** (p. 34)进一步了解验证。
    - 不用安装任何软件。本地控制台访问不使用验证。建议你只在安全环境下使用此选项。
    - 如果希望本地用户在 Dominion KX II 受 CC-SG 管理的情况下也访问它，选择 Ignore CC managed mode on local port（在本地端口忽略 CC 管理模式）复选框。

注意：如果最初选择在本地端口不忽略 CC 管理模式，但稍后要进行本地端口访问，必须在 CC-SG 上让设备不再受 CC-SG 管理，然后可以选择此复选框。



注意：为了在 Dominion KX II 受 CC-SG 管理的情况下使用标准本地端口和扩展本地端口，必须选择 Ignore CC managed mode on local port（在本地端口忽略 CC 管理模式）选项。如果希望本地用户在 Dominion KX II 受 CC-SG 管理的情况下通过标准本地端口或扩展本地端口访问它，选择 Ignore CC managed mode on local port（在本地端口忽略 CC 管理模式）复选框。也可以在设备受 CC-SG 管理的情况下使用直接设备访问。

---

13. 单击 OK（确定）按钮。

KX2-832 和 KX2-864 标准本地端口设置和扩展本地端口设置

KX2-832 和 KX2-864 有两个本地端口选项：标准本地端口和扩展本地端口。在 Remote Console 的 Port Configuration（端口配置）页上或 Local Console 的 Local Port Settings（本地端口设置）页上启用和禁用每个端口选项。参看***配置 Dominion KX II 本地端口设置*** (p. 185)了解详情。

默认启用标准本地端口，禁用扩展本地端口。如果要扩大本地端口的范围，启用扩展本地端口，用一根 5/5e/6 类电缆把 Paragon II UMT、EUST、UST 或 URKVMG 连接到 DKX2-832 或 DKX2-864。

注意：如果在 KX2-832 和 KX2-864 上启用扩展本地端口，但此端口没有连接任何东西，在通过本地端口切换到目标服务器时有 2-3 秒延迟。

必须具备管理员权限才能配置这些选项。如要访问端口，只需输入一次用户名和密码。在访问每个端口时不必再输入这些证书。

参看***规格*** (p. 251)一节，详细了解扩展本地端口支持的设备、距离规格和支持的 CIM。

KX2-832 和 KX2-864 连接限制

标准本地端口和扩展本地端口共享目标服务器访问。如果同时启用二者，标准本地端口和扩展本地端口共享键盘、视频和鼠标。二者同时连接目标服务器，同时与目标服务器断开。

如果禁用标准本地端口或扩展本地端口，端口将禁用键盘、视频和鼠标，显示一条消息说明本地端口被禁用了。



Ch 9 安全管理

在本章内

安全设置

可以在 **Security Settings（安全设置）页上指定登录限制、用户锁定、密码规则、加密和共享设置。**

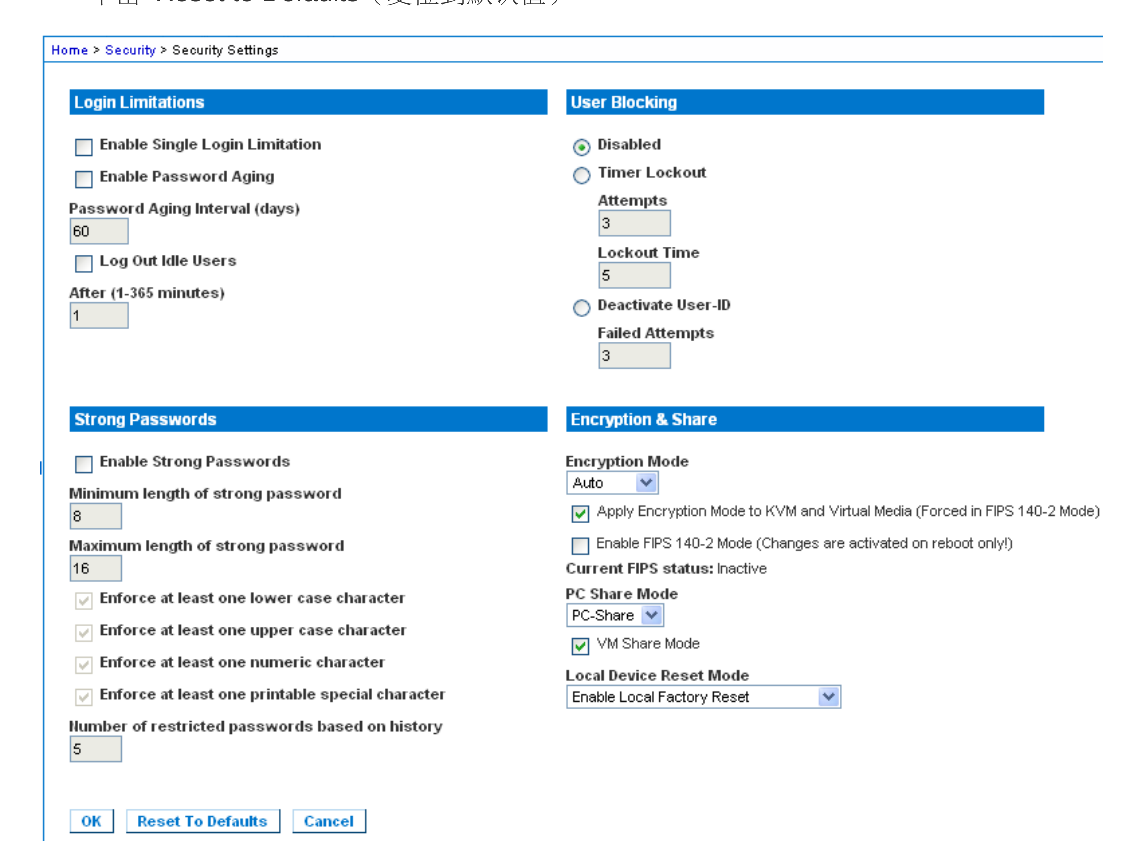
Raritan SSL 证书用于交换公共密钥和专用密钥，进一步增强安全。Raritan Web 服务器证书是自签名证书。Java 小程序证书是 VeriSign 签名的证书。加密确保信息不被他人偷听，这些证书确保你可以相信实体是 Raritan, Inc.。

▶ 配置安全设置：

1. 选择 Security（安全）> Security Settings（安全设置）。打开 Security Settings（安全设置）页。
2. 必要时更新***登录限制*** (p. 190)设置。
3. 适当更新***强密码*** (p. 191)设置。
4. 适当更新***用户锁定*** (p. 192)设置。
5. 适当更新加密和共享设置。
6. 单击 OK（确定）按钮。

复位到出厂前默认值：

- 单击 Reset to Defaults（复位到默认值）。



登录限制

可以用登录限制指定单点登录限制、密码有效期限制和闲置用户退出限制。

限制	说明
Enable single logon limitation（启用单点登录限制）	如果选择此选项，每个用户任何时候都只需登录一次。如果取消此选项，可以同时在几个客户机工作站上输入指定的用户名/密码组合访问设备。
Enable password aging（启用密码有效期）	如果选择此选项，所有用户必须根据在 Password Aging Interval（密码有效天数）字段里指定的天数定期更改密码。 如果选择 Enable Password Aging（启用密码有效期）复选框，启用此字段，必须填写此字段。输入



限制	说明
	必须在多少天之后更改密码。默认值是 60 天。
Log off idle users, After（在此之后退出闲置用户，1-365 分钟）	选择 Log off idle users（退出用户）复选框，在经过 After (1-365 minutes)（在此之后[1-365 分钟]）字段里指定的时间之后，自动断开用户。如果没有键盘活动或鼠标活动，注销所有会话和所有资源。但如果正在进行虚拟媒体会话，此会话不超时。 After（在此之后）字段用于设置在多久（分钟）之后退出闲置用户。如果选择 Log Out Idle Users（退出闲置用户）选项，启用此字段。最大可以输入 365 分钟作为字段值。

强密码

强密码给系统提供更安全的本地验证。可以利用强密码指定有效 Dominion KX II 本地密码的格式，例如最小长度、最大长度、要求的字符和密码历史保留期。

强密码要求用户创建的密码至少有 8 个字符，其中至少有一个字母字符和一个非字母字符（标点符号或数字）。此外，密码前四个字符不能与用户名相同。

如果选择此选项，强制应用强密码规则。如果用户密码不符合强密码标准的规定，自动要求用户在下次登录时更改密码。如果取消此选项，强制执行标准格式验证。如果选择此选项，启用下列字段，必须填写这些字段：

字段	说明
Minimum length of strong password（强密码最小长度）	密码至少要有 8 个字符。默认值是 8，最长为 63 个字符。
Maximum length of strong password（强密码最大长度）	默认值是 16，最长为 64 个字符。
Enforce at least one lower case character（强制至少有一个小写字符）	如果选择此复选框，密码至少要有一个小写字符。
Enforce at least one upper case character（强制至少有一个大写字符）	如果选择此复选框，密码至少要有一个大写字符。
Enforce at least one numeric character（强制至少有一个数字字符）	如果选择此复选框，密码至少要有一个数字字符。
Enforce at least one printable special character（强制至少有一个可打印特殊字符）	如果选择此复选框，密码至少要有一个可打印特殊字符。



字段	说明
Number of restricted passwords based on history（受限历史密码数）	此字段说明密码历史深度，即可以重复使用的旧密码数。范围是 1-12，默认值是 5。

用户锁定

User Blocking（用户锁定）选项指定用户锁定标准，在达到指定的登录失败次数之后禁止用户访问系统。

三个选项相互排斥：

选项	说明
Disabled（禁用）	默认选项。无论验证失败多少次，都不封锁用户。
Timer Lockout（定时器封锁）	在登录失败次数超过指定的次数之后，在指定的时间内拒绝用户访问系统。如果选择此选项，启用下列字段： ▪ Attempts（尝试次数）— 在封锁用户之前的登录失败次数。有效范围是 1-10，默认值是 3 次。 ▪ Lockout Time（封锁时间）— 用户锁定时间。有效范围是 1-1440 分钟，默认值是 5 分钟。 *注意：管理员用户不受定时器封锁设置的约束。*
Deactivate User-ID（停用用户 ID）	如果选择此选项，在达到在 Failed Attempts（失败次数）字段指定的登录失败次数之后，拒绝用户访问系统。 ▪ Failed Attempts（失败次数）— 在停用用户的用户 ID 之前的登录失败次数。如果选择 Deactivate User-ID（停用用户 ID）选项，启用此字段。有效范围是 1-10。

如果在指定的登录失败次数之后停用一个用户 ID，管理员必须在 User（用户）页上更改密码，选择 Active（活动）复选框激活该用户帐号。



加密和共享

可以用 Encryption & Share（加密和共享）设置指定所用的加密类型，PC 和虚拟媒体共享模式，以及在按 Dominion KX II Reset（复位）按钮时执行的复位的类型。

警告：如果选择浏览器不支持的加密模式，不能通过浏览器访问 Dominion KX II。

1. 在 Encryption Mode（加密模式）下拉列表上选择其中一个选项。在选择加密模式时显示警告消息，说明如果浏览器不支持选择的模式，不能连接 Dominion KX II。警告消息：在指定加密模式时，请确保浏览器支持此加密模式，否则不能连接 Dominion KX II。

加密模式	说明
自动	这是建议的选项。Dominion KX II 自动协商最高级加密。 *必须*选择 Auto（自动），设备和客户机才能成功协商符合 FIPS 规范的算法。
RC4	加密用户名、密码和 KVM 数据，包括用 RSA RC4 加密方法传输视频。这是 128 位 Secure Sockets Layer (SSL) 协议，在最初验证连接过程中，在 Dominion KX II 设备和远程 PC 之间提供专用通信通道。 如果启用 FIPS 140-2 模式并选择 RC4，将显示错误消息。在 FIPS 140-2 模式下不能使用 RC4。
AES-128	Advanced Encryption Standard (AES) 是 National Institute of Standards and Technology 制定的电子数据加密规范。128 是密钥长度。如果指定 AES-128，要确保浏览器支持它，否则不能建立连接。参看***检查浏览器的 AES 加密*** (p. 195)了解详情。
AES-256	Advanced Encryption Standard (AES) 是 National Institute of Standards and Technology 制定的电子数据加密规范。256 是密钥长度。如果指定 AES-256，要确保浏览器支持它，否则不能建立连接。参看***检查浏览器的 AES 加密*** (p. 195)了解详情。

注意：MPC 始终协商最高级加密，在 Encryption Mode（加密模式）没有设置为 Auto（自动）的情况下使其匹配。

注意：如果运行 Windows XP® SP2 操作系统，Internet Explorer 7 不能用 AES-128 加密算法远程连接 Dominion KX II。

2. Apply Encryption Mode to KVM and Virtual Media（将加密模式应用于 KVM 和虚拟媒体）。如果选择此选项，将选择的加密模式应用于 KVM 和虚拟媒体。在验证之后，KVM 数据和虚拟媒体数据也用 128 位加密模式传输。
3. 对于政府机构和其他需要高度安全的环境，选择 Enable FIPS 140-2（启用 FIPS 140-2）复选框启用 FIPS 140-2 模式。参看***启用 FIPS 140-2*** (p. 195)了解如何启用 FIPS 140-2。
4. PC Share Mode（PC 共享模式）。决定全局并发远程 KVM 访问，最多允许八个远程用户同时登录 Dominion KX II，同时通过该设备查看和控制同一台目标服务器。单击下拉列表选择下列选项之一：
   - Private（独占）— 无 PC 共享。这是默认模式。每台目标服务器每次均可由一个用户采用独占方式访问。
   - PC-Share（PC 共享）— KVM 目标服务器最多可让八个用户（管理员和非管理员）同时访问。但每个远程用户有相同的键盘和鼠标控制，如果一个用户不停止输入或移动鼠标，他们的控制可能不尽相同。
5. 必要时选择 VM Share Mode（虚拟媒体共享模式）。如果启用 PC-Share（PC 共享）模式，启用此选项。如果选择此选项，允许多个用户共享虚拟媒体，即几个用户可以访问同一个虚拟媒体会话。默认值是禁用。
6. 必要时选择 Disable Local Port Output（禁用本地端口输出）复选框。如果选择此选项，本地端口没有视频输出。此设置仅适用于 KX2 832 和 KX2 864。如果使用智能卡读卡器，*必须*禁用本地端口。
7. 必要时选择 Local Device Reset Mode（本地设备复位模式）。此选项指定在按（设备背面的）硬件 Reset（复位）按钮时，要执行哪些操作。参看用复位按钮复位 Dominion KX II 了解详情。选择下列选项之一：

本地设备复位模式	说明
Enable Local Factory Reset（启用本地出厂复位，默认值）	让 Dominion KX II 设备恢复出厂前默认值。
Enable Local Admin Password Reset（启用本地管理员密码复位）	只复位本地管理员密码。让密码恢复到 raritan。
Disable All Local	不执行复位操作。



本地设备复位模式	说明
Resets（禁用所有本地复位）	

注意：在使用 P2CIM-AUSBDUAL 或 P2CIM-APS2DUAL 把目标服务器连接到两台 Dominion KX II 时，如果需要独占访问目标服务器，必须把两台 KVM 切换器的 PC Share（PC 共享）模式设置为 Private（独占）。

参看***支持的 Paragon CIMS 和配置*** (参看 "***支持的 Paragon CIM 和配置***" p. 261)，进一步了解如何一起使用 Paragon CIM 和 Dominion KX II。

检查浏览器的 AES 加密

Dominion KX II 支持 AES-256。如果不知道浏览器是否使用 AES，可以向浏览器开发商咨询，或者给浏览器设置要检查的加密方法，然后访问 https://www.fortify.net/sslcheck.html 网站。此网站检测浏览器使用的加密方法，并显示检测报告。

注意：IE6 不支持 AES 128 位或 256 位加密。

AES 256 要求和支持的配置

只有下列网络浏览器支持 AES 256 位加密：

- Firefox® 2.0.0.x 和 3
- Mozilla® 1.7.13
- Internet Explorer® 7 和 8

除了浏览器支持，AES 256 位加密还要求安装 Java™ Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files。

各种 JRE™ 的 Jurisdiction Files 可以在下列网站的 other downloads（其他下载）部分找到：

- JRE1.6 - http://java.sun.com/javase/downloads/index_jdk5.jsp

启用 FIPS 140-2

对于政府机构和其他需要高度安全的环境，可能想启用 FIPS 140-2 模式。Dominion KX II 使用在 Linux® 平台上运行的嵌入式 FIPS 140-2 认证加密模块，按 FIPS 140-2 实现指导原则第 G.5 节指导原则进行加密。在启用此模式之后，必须在内部生成专用密钥，以便生成 SSL 证书；专用密钥不能下载或导出。

▶ **启用 FIPS 140-2：**

1. 访问 Encryption & Share（加密和共享）页（参看***加密和共享*** (p. 193)）。



2. 在 Security Settings（安全设置）页的 Encryption & Share（加密和共享）部分选择 Enable FIPS 140-2（启用 FIPS 140-2）复选框，启用 FIPS 140-2 模式。将在 FIPS 140-2 模式下把 FIPS 140-2 批准的算法用于外部通信。用 FIPS 加密模块加密 KVM 会话流量，包括视频数据、键盘数据、鼠标数据、虚拟媒体数据和智能卡数据。
3. Reboot the Dominion KX II.要求

   在激活 FIPS 模式之后，屏幕左面板的 Device Information（设备信息）部分显示 FIPS Mode: Enabled（FIPS 模式：启用）。

   为了增强安全，在激活 FIPS 模式之后还可以创建新证书签名请求。此请求用所需的密钥创建。在签名证书之后上载证书，或者创建一个自签名证书。SSL Certificate（SSL 证书）状态从 Not FIPS Mode Compliant（不符合 FIPS 模式）更新为 FIPS Mode Compliant（符合 FIPS 模式）。

   在激活 FIPS 模式之后，密钥文件不能下载或上载。最新创建的 CSR 在内部与密钥文件关联。此外，CA 签发的 SSL 证书及其专用密钥并不包括在备份文件的全恢复中。不能从 Dominion KX II 导出密钥。

FIPS 140-2 支持要求

Dominion KX II 支持使用 FIPS 140-20 批准的加密算法。这样，当客户机配置为仅 FIPS 140-2 模式时，SSL 服务器和客户机可以成功协商加密会话所用的加密算法。

下面是 FIPS 140-2 和 Dominion KX II 使用建议：

Dominion KX II

- 在 Security Settings（安全设置）页上把 Encryption & Share（加密和共享）设置为 Auto（自动）。参看加密和共享。

Microsoft 客户机

- 应该在客户计算机和 Internet Explorer 上禁用 FIPS 140-2。

► **在 Windows 客户机上启用 FIPS 140-2：**

1. 选择 Control Panel（控制面板）> Administrative Tools（管理工具）> Local Security Policy（本地安全策略），打开 Local Security Settings（本地安全设置）对话框。
2. 在导航树上选择 Select Local Policies（选择本地策略）> Security Options（安全选项）。
3. 启用 System Cryptography: Use FIPS compliant algorithms for encryption, hashing and signing（系统加密：把符合 FIPS 规范的算法用于加密、散列和签名）。



4. 重新启动客户计算机。

► **在 Internet Explorer 上启用 FIPS 140-2：**

1. 在 Internet Explorer 上选择 Tools（工具）> Internet Options（Internet 选项），单击 Advanced（高级）选项卡。
2. 选择 Use TLS 1.0（使用 TLS 1.0）复选框。
3. 重新启动浏览器。

配置 IP 访问控制

可以用 IP 访问控制来控制对 Dominion KX II 的访问。设置一个全局访问控制表 (ACL)，确保设备不响应来自被禁 IP 地址的数据包。IP 访问控制是全局性的，影响整个 Dominion KX II，但也可以在组一级控制对设备的访问。参看***基于组的 IP 访问控制表*** (p. 112)，进一步了解组级控制。

重要说明：Dominion KX II 本地端口使用的 IP 地址是 127.0.0.1。在创建 IP 访问控制表时，127.0.0.1 不应在被禁的 IP 地址范围内，否则不能访问 Dominion KX II 本地端口。

► **使用 IP 访问控制：**

1. 选择 Security（安全）> IP Access Control（IP 访问控制），打开 IP Access Control（IP 访问控制）页。打开 IP Access Control（IP 访问控制）页。
2. 选择 Enable IP Access Control（启用 IP 访问控制）复选框启用 IP 访问控制和本页上的其他字段。
3. 选择 Default Policy（默认策略）。这是针对不在指定范围内的 IP 地址执行的操作。
   - Accept（接受）— 允许 IP 地址访问 Dominion KX II 设备。
   - Drop（拒绝）— 拒绝 IP 地址访问 Dominion KX II 设备。

注意：同时支持 IPv4 地址和 IPv6 地址。

► **添加（附加）规则：**

1. 在 IPv4/Mask（IPv4/子网掩码）字段或 IPv6/Prefix Length（IPv6/前缀长度）字段里输入 IP 地址和子网掩码。

注意：IP 地址应该采用 CIDR（Classless Inter-Domain Routing 表示法，前面 24 位用作网络地址）格式输入。

2. 在 Policy（策略）下拉列表上选择策略。
3. 单击 Append（附加）。此规则被添加到规则列表末尾。



插入规则：

1. 输入规则编号。在使用 Insert（插入）命令时，需要规则编号。
2. 在 IPv4/Mask（IPv4/子网掩码）字段或 IPv6/Prefix Length（IPv6/前缀长度）字段里输入 IP 地址和子网掩码。
3. 在 Policy（策略）下拉列表上选择策略。
4. 单击 Insert（插入）。如果输入的规则编号与现有规则编号相同，将新规则放在现有规则前面，列表上的所有规则向下移。

提示：规则编号便于你更好地控制规则创建顺序。

替换规则：

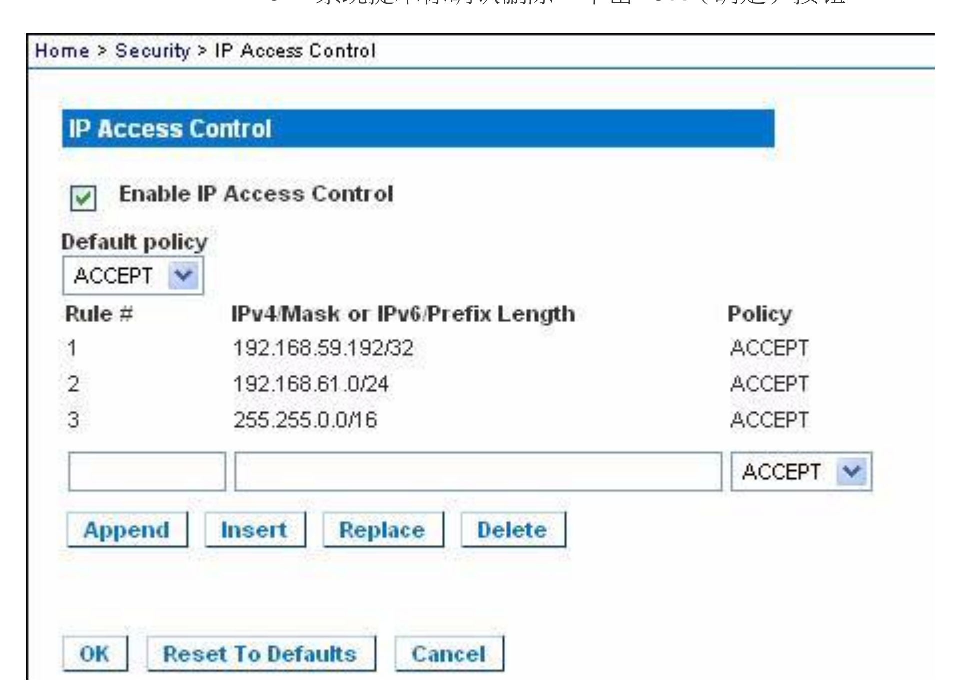
1. 指定要替换的规则编号。
2. 在 IPv4/Mask（IPv4/子网掩码）字段或 IPv6/Prefix Length（IPv6/前缀长度）字段里输入 IP 地址和子网掩码。
3. 在 Policy（策略）下拉列表上选择策略。
4. 单击 Replace（替换）。新规则取代规则编号相同的旧规则。

删除规则：

1. 指定要删除的规则编号。
2. 单击 Delete（删除）按钮。



3. 系统提示你确认删除。单击 OK（确定）按钮。



SSL 证书

Dominion KX II 将 Secure Socket Layer (SSL) 协议用于它和相连客户机之间的所有加密网络流量。在建立连接时，Dominion KX II 必须采用加密证书向客户机表明自己的身份。

可以生成证书签名请求 (Certificate Signing Request, CSR)，将验证中心签名的证书安装在 Dominion KX II 上。验证中心验证 CSR 发出人的身份。验证中心然后返回一个证书，包含它给发出人的签名。经知名验证中心签名的证书用于确保证书持有人的身份。

Certificate Signing Request (CSR)

Common name

Organizational unit

Organization

Locality/City

State/Province

Country (ISO code)

Email

Challenge password

Confirm Challenge password

Key length (bits)

1024 *

Create

* Stored value is equal to the default.

▶ 创建和安装 SSL 证书：

1. 选择 Security（安全）> SSL Certificate（SSL 证书）。
2. 填写下列字段：



a. Common name（公用名）— Dominion KX II 被安装在用户网络上之后，它的网络名称（通常是全限定域名）。它与用网络浏览器访问 Dominion KX II 所用的名称相同，但没有 http:// 前缀。如果在此指定的名称与实际网络名称不相同，在用 HTTPS 访问 Dominion KX II 时，浏览器会弹出安全警告。

b. Organizational unit（机构单位）— 此字段用于指定 Dominion KX II 归机构的哪个部门所有。

c. Organization（机构）— Dominion KX II 所属机构的名称。

d. Locality/City（地区/城市）— 机构所在的城市。

e. State/Province（州/省）— 机构所在的州或省。

f. Country (ISO code)（国家，ISO 代码）— 机构所在的国家。这是双字母 ISO 代码，例如 DE 表示德国，US 表示美国。

g. Challenge Password（挑战密码）— 某些验证中心需要用挑战密码对随后的证书变动进行授权（例如取消证书）。此密码的最小长度是四个字符。

h. Confirm Challenge Password（确认挑战密码）— 确认挑战密码。

i. Email（电子邮件）— 负责 Dominion KX II 及其安全的联系人的电子邮件地址。

j. Key length（密钥长度）— 生成的密钥位数。默认值是 1024。

3. 单击 Create（创建）按钮生成证书签名请求 (CSR)。

▶ 下载一个 CSR 证书：

1. 可以单击 Download（下载）按钮，下载 CSR 和在创建它时所用的专用密钥所在的文件。

注意：CSR 与专用密钥文件相匹配，应作相应的处理。如果签名证书不匹配在生成原始 CSR 时所用的专用密钥，证书没有任何意义。这适用于上载和下载 CSR 和专用密钥文件。

2. 将保存的 CSR 发送到验证中心进行验证。你将收到来自验证中心的新证书。

▶ 上载 CSR：

1. 单击 Upload（上载）按钮，将证书上载到 Dominion KX II。

注意：CSR 与专用密钥文件相匹配，应作相应的处理。如果签名证书不匹配在生成原始 CSR 时所用的专用密钥，证书没有任何意义。这适用于上载和下载 CSR 和专用密钥文件。

Certificate Signing Request (CSR)

The following CSR is pending:

```
countryName                = US
stateOrProvinceName        = DC
localityName               = Washington
organizationName           = ACME Corp.
organizationalUnitName     = Marketing Dept.
commonName                 = John Doe
emailAddress               = johndoe@acme.com
```

Download Delete

Certificate Upload

SSL Certificate File

Browse...

Upload

在完成这三个步骤之后，Dominion KX II 有了自己的证书，可以用此证书向客户机表明自己的身份了。

重要说明 :如果销毁了 Dominion KX II 上的 CSR, 没有办法把它找回来！如果误删除了证书，必须重复上述三个步骤。为了避免出现这种情况，可以使用下载功能，保留 CSR 及其专用密钥的副本。

安全提示

Dominion KX II 使你能给 Dominion KX II 登录过程增加安全提示。此功能要求用户在访问 Dominion KX II 之前接受或拒绝安全协议。在用户用自己的登录证书访问 Dominion KX II 之后，Restricted Service Agreement（有限服务协议）对话框显示在安全提示上输入的信息。

安全提示的标题和措词可以定制，也可以使用默认文本。还可以配置安全提示，要求用户在访问 Dominion KX II 之前接受安全协议，还是只在登录过程中显示安全协议。如果启用接受或拒绝功能，把用户所做的选择记录在审计日志里。

▶ 配置安全提示：

1. 单击 Security（安全）> Banner（提示）打开 Banner（提示）页。
2. 选择 Display Restricted Service Banner（显示有限服务提示）启用此功能。
3. 如果要求用户在继续登录过程之前确认提示，选择 Require Acceptance of Restricted Service Banner（要求接受有限服务提示）。用户选择一个复选框，即可确认提示。如果不启用此设置，只在用户登录后显示安全提示，不要求用户确认提示。
4. 必要时更改提示的标题。此信息作为提示的一部分给用户显示。最长可以使用 64 个字符。

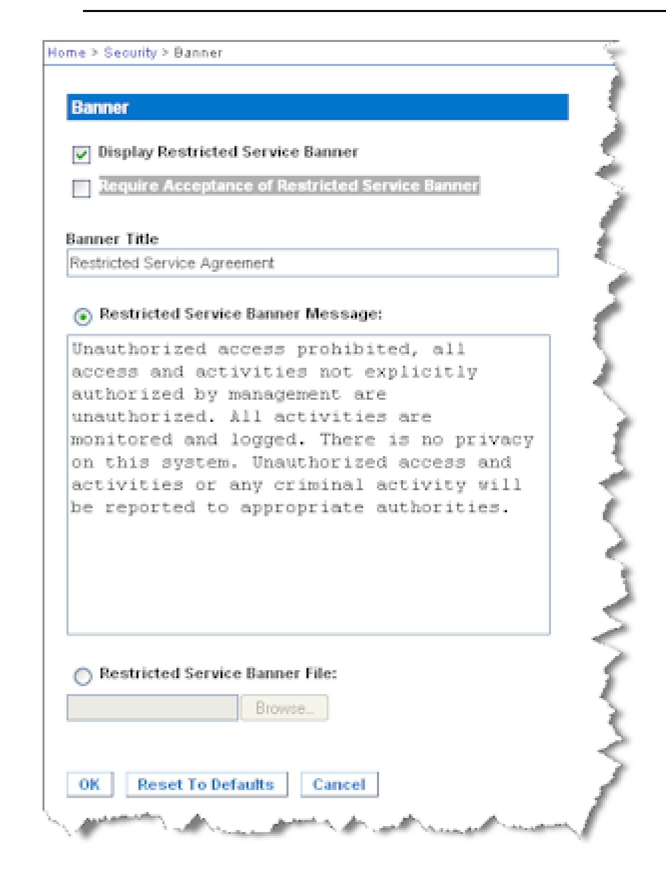


5. 编辑 Restricted Services Banner Message（有限服务提示消息）文本框里的信息。最多可以在文本文件里输入或上载 6000 个字符。为此，执行下列操作之一：

   a. 用人工法把文字输入文本框。单击 OK（确定）按钮。

   b. 选择 Restricted Services Banner File（有限服务提示文件）单选按钮，用 Browse（浏览）功能找到并上载 .txt 文件，即可上载信息。单击 OK（确定）按钮。在上载文件之后，Restricted Services Banner Message（有限服务提示消息）文本框显示文件里的文字。

注意：不能在本地端口上载文本文件。





Ch 10　维护

在本章内

审计日志

给 Dominion KX II 系统事件创建一个日志。

▶ 查看 Dominion KX II 审计日志：

1. 选择 Maintenance（维护）> Audit Log（审计日志）。打开 Audit Log（审计日志）页。

   Audit Log（审计日志）页按日期和时间显示事件（最新的事件列在前面）。审计日志显示下列信息：

   - Date（日期）— 事件发生日期和时间（24 小时时钟）。
   - Event（事件）— Event Management（事件管理）页列出的事件名称。
   - Description（说明）— 事件详细说明。

▶ 保存审计日志：

注意：只能在 Dominion KX II Remote Console 上保存审计，在 Dominion KX II Local Console 上不能保存。

1. 单击 Save to File（保存到文件）按钮。打开 Save File（保存文件）对话框。
2. 选择希望的文件名和保存位置，单击 Save（保存）按钮。采用指定的名称和位置，将审计文件保存在本地客户机上。

▶ 审计日志翻页：

- 使用 [Older]（较旧）和 [Newer]（较新）链接。



设备信息

Device Information（设备信息）页显示 Dominion KX II 设备和所用 CIM 的详细信息。如果必须联系 Raritan 技术支持部门，这些信息很有用。

▶ 查看 Dominion KX II 和 CIM 信息：

- 选择 Maintenance（维护）> Device Information（设备信息）。打开 Device Information（设备信息）页。

显示下列 Dominion KX II 信息：

- 型号
- Hardware Revision（硬件版本）
- Firmware Version（固件版本）
- Serial Number（序列号）
- MAC Address（MAC 地址）

显示所用的 CIM 的下列信息：

- Port (number)（端口号）
- Name（名称）
- Type of CIM（CIM 类型）— DCIM、PCIM、电源条或虚拟媒体
- Firmware Version（固件版本）
- Serial Number（序列号）

Home > Maintenance > Device Information   Logout

Device Information

Model:	D232
Hardware Revision:	0x48
Firmware Version:	2.0.20.5.6882
Serial Number:	HKB7500230
MAC Address:	00:0d:5d:03:cc:b5

CIM Information

▲ Port	Name	Type	Firmware Version	Serial Number
1	Dominion	VM	2A5D	HUW7250867
8	PwrStrip	PowerStrip	00B4	PQ16A00058



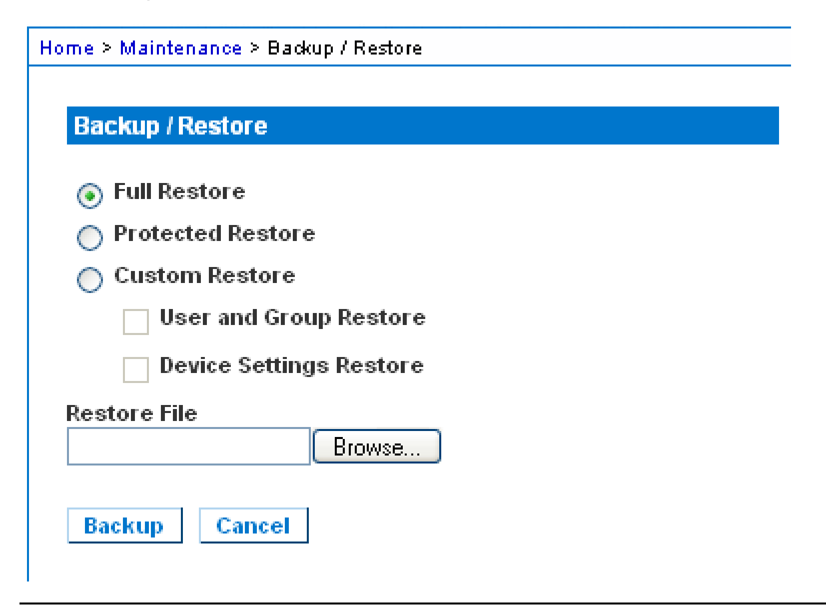
备份和恢复

可以在 Backup/Restore（备份/恢复）页上备份和恢复 Dominion KX II 的设置和配置。

除了用备份和恢复功能增强业务连续性，还可以将它用作节省时间的方法。例如备份使用中的 Dominion KX II 的用户配置设置，将这些配置恢复到新的 Dominion KX II 上，可以通过另一台 Dominion KX II 给团队提供访问。还可以设置一台 Dominion KX II，将它的配置复制到多台 Dominion KX II 设备上。

▶ 访问备份/恢复页：

- 选择 Maintenance（维护）> Backup/Restore（备份/恢复）。打开 Backup/Restore（备份/恢复）页。



注意：备份功能始终完整备份整个系统。恢复既可以是完整恢复，也可以是部分恢复，取决于你的选择。

▶ 如果使用 **FireFox®、Internet Explorer® 5 或更低版本备份 Dominion KX II：**

1. 单击 Backup（备份）。打开 File Download（文件下载）对话框。
2. 单击 Save（保存）按钮。打开 Save As（另存为）对话框。
3. 选择保存位置，指定文件名，单击 Save（保存）按钮。打开 Download Complete（完整下载）对话框。



4. 单击 Close（关闭）按钮。采用指定的名称和位置，将备份文件保存在本地客户机上。

▶ 如果使用 Internet Explorer 6 或更高版本备份 Dominion KX II：

1. 单击 Backup（备份）。打开 File Download（文件下载）对话框，对话框上有 Open（打开）按钮。不要单击 Open（打开）按钮。

   在使用 IE 6 和更高版本时，把 IE 用作打开文件的默认应用程序，所以系统提示你打开问题，而不是保存文件。如要避免出现这种情况，必须把打开文件所用的默认应用程序更改为 Wordpad。

2. 为此：
   a. 保存备份文件。采用指定的名称和位置，将备份文件保存在本地客户机上。
   b. 在保存文件之后找到它，用右键单击它。单击 Properties（属性）。
   c. 单击 General（常规）选项卡上的 Change（更改），选择 Wordpad。

▶ 恢复 Dominion KX II：

> 警告：在将 Dominion KX II 恢复到较早版本时务必谨慎。将恢复在备份文件时使用的用户名和密码。如果不记得旧管理用户名和密码，不能访问 Dominion KX II。
>
> 此外，如果在备份时使用不同的 IP 地址，也恢复该 IP 地址。如果设备配置使用 DHCP，可能只有在访问本地端口检查更新之后的 IP 地址时，才要执行此操作。

1. 选择要执行的恢复类型：



- Full Restore（全恢复）— 完整恢复整个系统。通常用于传统备份和恢复。
- Protected Restore（保护恢复）— 除了 IP 地址、名称等设备特定的信息，全部恢复。如果选择此选项，可以设置一台 Dominion KX II，将它的配置复制到多台 Dominion KX II 设备上。
- Custom Restore（定制恢复）— 如果选择此选项，可以选择 User and Group Restore（用户和组恢复）和/或 Device Settings Restore（设备设置恢复）。
    - User and Group Restore（用户和组恢复）— 此选项只包括用户信息和组信息。此选项不恢复证书文件和专用密钥文件。用此选项迅速恢复不同 Dominion KX II 上的用户。
    - Device Settings Restore（设备设置恢复）— 此选项只包括设备设置，例如电源关联、USB 配置文件、与刀片服务器机箱有关的配置参数和端口组指定。用此选项迅速复制设备信息。

1. 单击 Browse（浏览）按钮。打开 Choose File（选择文件）对话框。
2. 找到并选择相应的备份文件，单击 Open（打开）按钮。Restore File（恢复文件）字段列出选择的文件。
3. 单击 Restore（恢复）按钮。根据选择的恢复类型恢复配置。



USB 配置文件管理

可以在 USB Profile Management（USB 配置文件管理）页上上载 Raritan 技术支持部门提供的定制配置文件。在标准配置文件不能满足目标服务器配置的要求时，这些配置文件可以满足它们的要求。Raritan 技术支持部门提供定制配置文件，与你一起验证解决方案是否满足目标服务器的特定要求。

▶ **访问 USB 配置文件管理页：**

- 选择 Maintenance（维护）> USB Profile Management（USB 配置文件管理）。打开 USB Profile Management（USB 配置文件管理）页。



▶ **将定制配置文件上载到 Dominion KX II：**

1. 单击 Browse（浏览）按钮。打开 Choose File（选择文件）对话框。
2. 找到并选择相应的定制配置文件，单击 Open（打开）按钮。USB Profile File（USB 配置文件）字段列出选择的文件。
3. 单击 Upload（上载）按钮。上载定制配置文件，Profile（配置文件）表显示该定制配置文件。

注意：如果在上载过程中显示错误消息或警告消息（覆盖现有的定制配置文件），可以单击 Upload（上载）按钮继续上载，或者单击 Cancel（取消）按钮取消上载。

▶ **将定制配置文件从 Dominion KX II 上删除掉：**

1. 选择要删除的定制配置文件所在表行对应的复选框。
2. 单击 Delete（删除）按钮。删除定制配置文件，Profile（配置文件）表不再显示该定制配置文件。

可以将定制配置文件从系统上删除掉，虽然它仍然被指定为活动配置文件。这样会中断正在进行的任何虚拟媒体会话。

处理配置文件名称冲突

在执行固件升级时，定制 USB 配置文件和标准 USB 配置文件之间可能会发生命名冲突。如果创建一个定制配置文件，并将它添加到标准配置文件列表上，但它的名称与作为固件升级组成部分下载的新 USB 配置文件相同，就会发生这种情况。

如果发生这些情况，现有的定制配置文件被标记为 old_。例如假如创建了名为 GenericUSBProfile5 的定制配置文件，但在固件升级过程中下载一个同名配置文件，就将现有文件命名为 old_GenericUSBProfile5。

必要时可以删除现有配置文件。参看 ***USB 配置文件管理*** (p. 209)了解详情。

升级 CIM

通过这个功能可以使用存储在 Dominion KX II 内存里的 CIM 固件来升级 CIM。在用 Firmware Upgrade（固件升级）页升级设备固件时，通常同时升级 CIM。

为了使用 USB 配置文件，必须使用安装了最新固件的 D2CIM-VUSB 或 D2CIM-DVUSB。尚未升级固件的 VM-CIM 支持许多配置（Windows®、键盘、鼠标、CD-ROM 和可拆卸驱动器），但不能使用那些针对特定目标服务器配置优化过的配置文件。除此之外，为了访问 USB 配置文件，还应该将现有 VM-CIM 的固件升级到最新版本。在升级现有 VM-CIM 之前，它们具备的功能相当于 Generic 配置文件的功能。

注意：在本页只能升级 D2CIM-VUSB。

▶ 用 Dominion KX II 内存升级 CIM：

1. 选择 Maintenance（维护）> CIM Firmware Upgrade（CIM 固件升级）。打开 CIM Upgrade（CIM 升级）页。

   显示 Port (number)（端口号）、Name（名称）、Type（类型）、Current CIM Version（当前 CIM 版本）和 Upgrade CIM Version（升级 CIM 版本），CIM 标识一目了然。

2. 选择要升级的每个 CIM 对应的 Selected（选择）复选框。

   提示：用 Select All（全选）按钮和 Deselect All（全部取消）按钮迅速选择或取消所有 CIM。

3. 单击 Upgrade（升级）按钮。系统提示你确认升级。



4. 单击 OK（确定）按钮继续升级。在升级过程中显示进度条。每个 CIM 的升级时间不超过 2 分钟。

升级固件

用 Firmware Upgrade（固件升级）页升级 Dominion KX II 和所有相连 CIM 的固件。本页只能在 Dominion KX II Remote Console 上打开。

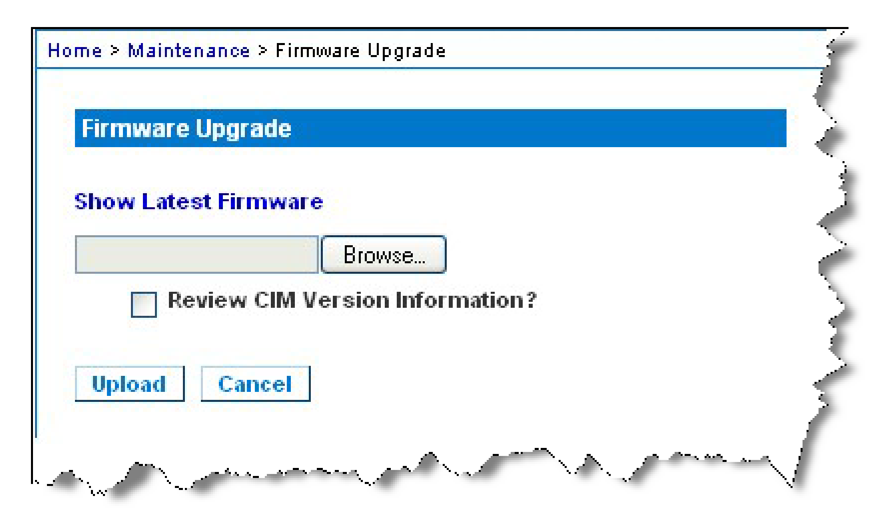
重要说明：在升级过程中切勿关闭 Dominion KX II 设备或断开 CIM，否则可能会损坏设备或 CIM。

▶ 升级 Dominion KX II 设备：

1. 在 ***Raritan 网站 http://www.raritan.com***的 Firmware Upgrades（固件升级）网页上找到合适的 Raritan 固件分发文件 (*.RFP)。
2. 解压文件。请在升级之前仔细阅读固件 ZIP 文件中的所有说明。

   注意：在上载之前将固件更新文件复制到本地 PC 上。切勿从网络驱动器上加载文件。

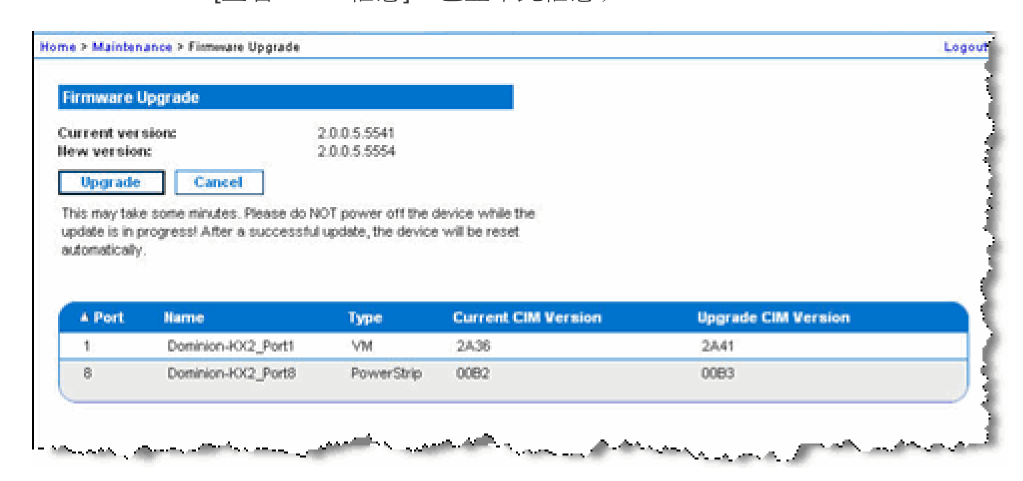
3. 选择 Maintenance（维护）> Firmware Upgrade（固件升级）。打开 Firmware Upgrade（固件升级）页。



4. 单击 Browse（浏览）按钮，找到升级文件解压目录。
5. 如果希望显示正在使用的 CIM 的版本信息，选择 Review CIM Version Information?（是否查看 CIM 版本信息？）复选框。



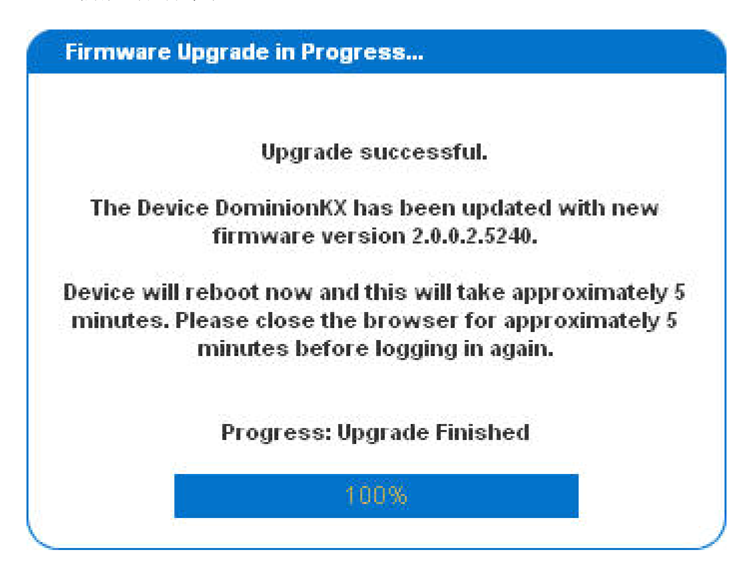
6. 单击 Firmware Upgrade（固件升级）页上的 Upload（上载）。显示升级信息和版本号信息，等待你确认（如果选择了 Review CIM Information[查看 CIM 信息]，也显示此信息）：



注意：此时退出联网用户，禁止新登录。

---

7. 单击 Upgrade（升级）。等待升级完成。在升级过程中显示状态信息和进度条。在升级结束之后，设备重新启动（发出一声蜂鸣声，表示重新启动结束）。



8. 在提示时关闭浏览器，等待大约五分钟即可再次登录 Dominion KX II。



参看 **KVM 和串行访问客户机指南**中的“升级设备固件”，了解如何用 Multi-Platform Client 升级设备固件。

注意：不支持通过调制解调器进行固件升级。

注意：如果使用级联配置，用基础 Dominion KX II 设备访问多台其他级联设备，单击基础设备名称左边的展开箭头图标 ，在 Port Access（端口访问）页上查看级联设备。如果有大量用户组，在升级固件过程中可能显示内存太小。如果显示此错误消息，可以重新启动设备，再次进行升级。如果在重新启动设备之后仍然显示此错误消息，可以在基础设备上禁用分层，再次进行升级。



升级历史记录

Dominion KX II 提供有关在 Dominion KX II 和相连的 CIM 上进行的升级的信息。

▶ 查看升级历史记录：

- 选择 Maintenance（维护）> Upgrade History（升级历史记录）。打开 Upgrade History（升级历史记录）页。

显示有关已进行的 Dominion KX II 升级的信息、升级最终状态、开始时间和结束时间、旧固件版本和当前固件版本。同时显示有关 CIM 的信息，单击升级对应的显示链接即可获得这些信息。显示下列 CIM 信息：

- Type（类型）— CIM 的类型。
- Port（端口）— CIM 连接的端口。
- User（用户）— 执行升级的用户。
- IP — 固件所在位置的 IP 地址。
- Start Time（开始时间）— 升级开始时间。
- End Time（结束时间）— 升级结束时间。
- Previous Version（旧版本）— CIM 旧固件版本。
- Upgrade Version（升级版本）— 当前 CIM 固件版本。
- CIM — 升级的 CIM。
- Result（结果）— 升级结果（成功或失败）。



Type	User	IP	Start Time	End Time	Previous Version	Upgrade Version	CIM's	Result
Full Firmware Upgrade	admin	192.168.59.63	June 16, 2008 14:15	June 16, 2008 14:23	2.0.20.5.6882	2.0.20.5.6926	show	Successful
Full Firmware Upgrade	admin	192.168.59.80	May 22, 2008 17:49	May 22, 2008 17:56	2.0.20.1.6853	2.0.20.5.6882	show	Successful

重新启动

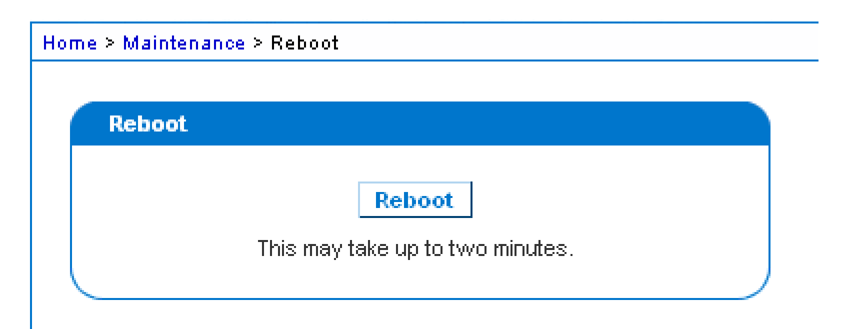
Reboot（重新启动）页提供一种安全的受控方法，可以在此重新启动 Dominion KX II。这是建议的重新启动方法。

重要说明：必须关闭所有 KVM 连接和串行连接，必须退出所有用户。

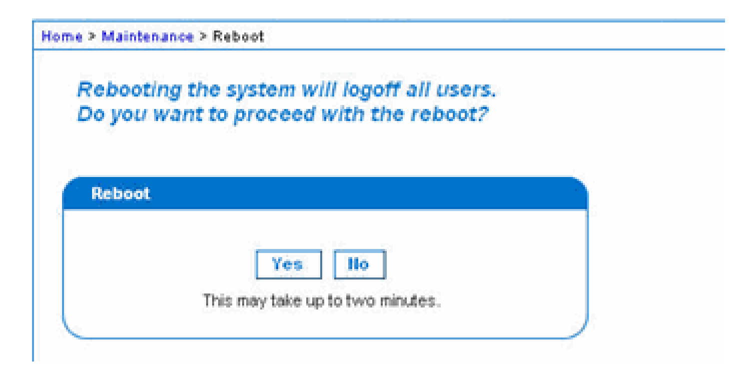


▶ 重新启动 Dominion KX II：

1. 选择 Maintenance（维护）> Reboot（重新启动）。打开 Reboot（重新启动）页。



2. 单击 Reboot（重新启动）。系统提示你确认操作。单击 Yes（是）按钮继续重新启动。



停止 CC-SG 管理

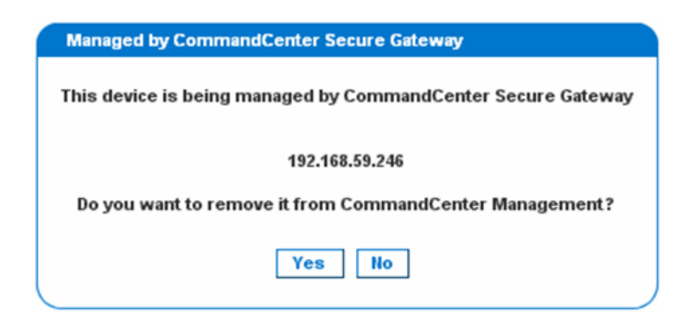
当 Dominion KX II 受 CC-SG 管理时，如果尝试直接访问该设备，系统通知你它受 CC-SG 管理。

如果通过 CC-SG 管理 Dominion KX II，CC-SG 和 Dominion KX II 之间的连接在指定的超时间隔（通常是 10 分钟）之后断开，可以在 Dominion KX II 控制台上终止 CC-SG 管理会话。

注意：必须具备适当的权限，才能终止 Dominion KX II CC-SG 管理。此外，除非当前用 CC-SG 管理 Dominion KX II，否则不显示 Stop CC-SG Management（停止 CC-SG 管理）选项。

▶ 停止 Dominion KX II CC-SG 管理：

1. 单击 Maintenance（维护）> Stop CC-SG Management（停止 CC-SG 管理）。显示一条消息，说明设备现在受 CC-SG 管理。同时显示一个选项，可以用此选项让设备不再受 CC-SG 管理。



2. 单击 Yes（是）按钮，让设备不再受 CC-SG 管理。显示一条确认消息，请你确认不再让 CC-SG 管理设备。

Managed by CommandCenter Secure Gateway

Confirming remove of the device from CommandCenter (192.168.59.246) Management.

Do you really want to remove this device from CommandCenter Management?

Yes No

3. 单击 Yes（是）按钮，让设备不再受 CC-SG 管理。在终止 CC-SG 管理之后，显示一条确认消息。

Managed by CommandCenter Secure Gateway

Stop CC-SG Management is successful. The device is no longer under CC-SG Management mode.

Ok

Ch 11 Diagnostics（诊断）

在本章内

网络接口页

Dominion KX II 显示网络接口状态信息。

▶ 查看网络接口信息：

- 选择 Diagnostics（诊断）> Network Interface（网络接口）。打开 Network Interface（网络接口）页。

显示下列信息：

- Ethernet 接口工作还是停止。
- 是否可以对网关执行 ping 命令。
- 当前活动的 LAN 端口。

▶ 刷新这些信息：

- 单击 Refresh（刷新）按钮。

网络统计数据页

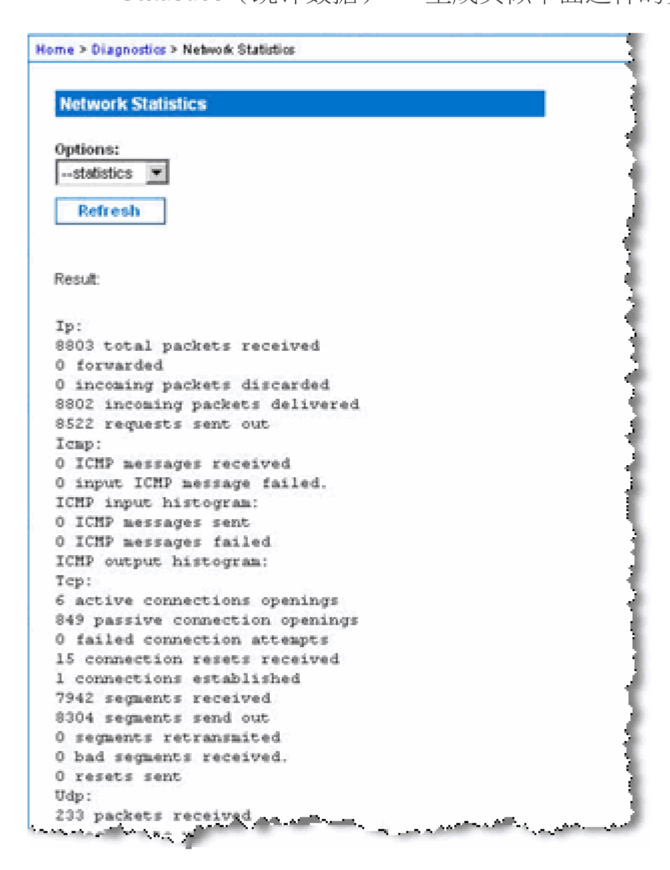
Dominion KX II 显示网络接口统计数据。

▶ 查看网络接口统计数据：

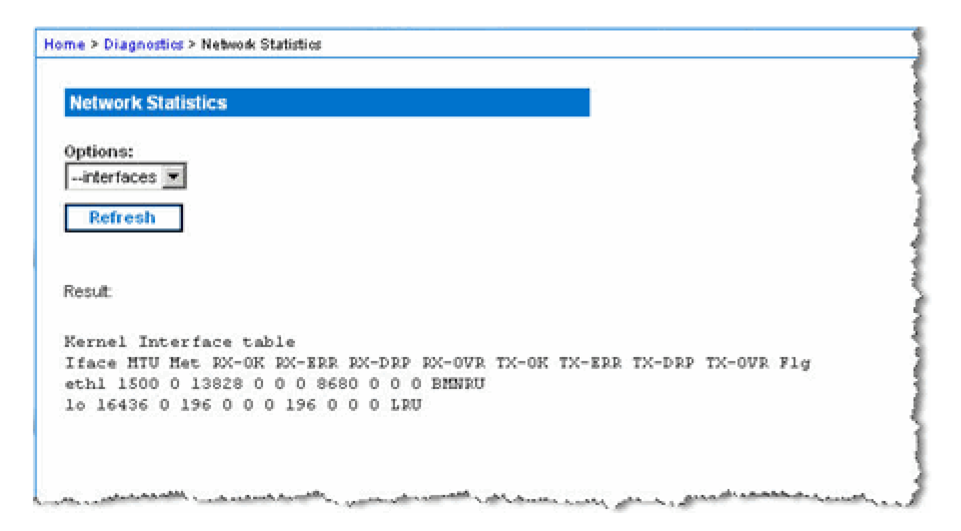
1. 选择 Diagnostics（诊断）> Network Statistics（网络统计数据）。打开 Network Statistics（网络统计数据）页。
2. 在 Options（选项）下拉列表上选择适当的选项：



- Statistics（统计数据）— 生成类似下面这样的页面。

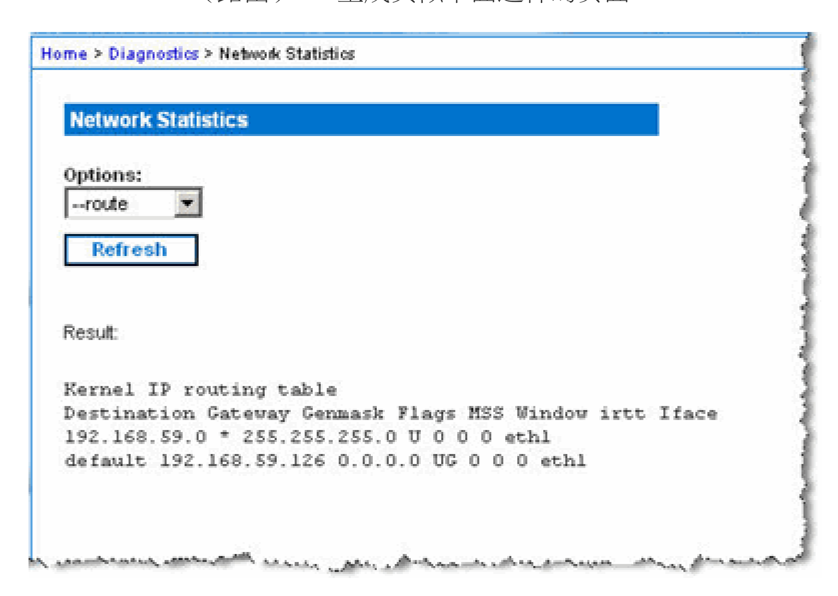


- Interfaces（接口）— 生成类似下面这样的页面。





- Route（路由）— 生成类似下面这样的页面。



3. 单击 Refresh（刷新）按钮。Result（结果）字段显示相关信息。

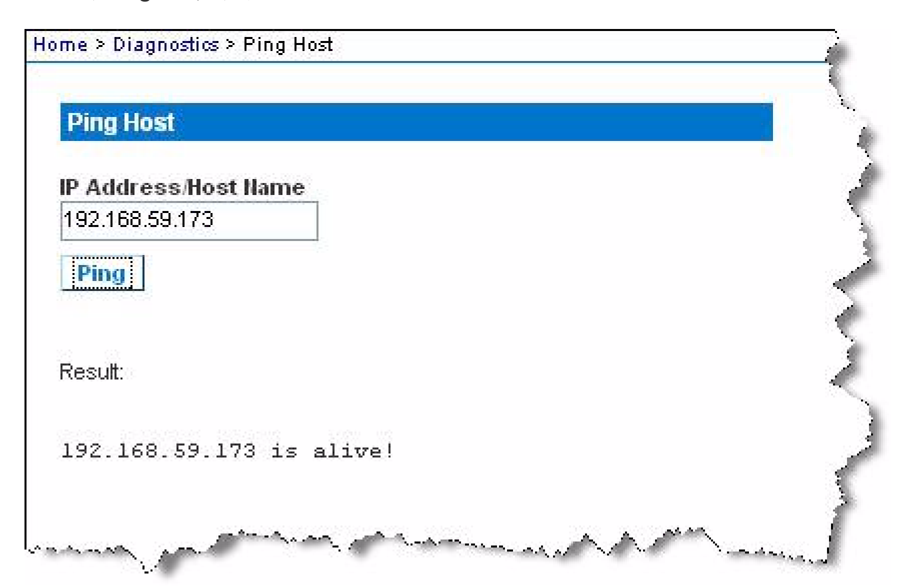


Ping 主机页

Ping 是网络工具，用于测试特定主机或 IP 地址是否可以通过 IP 网络访问。可以在 Ping Host（Ping 主机）页上确定目标服务器或另一台 Dominion KX II 是否可访问。

▶ Ping 主机：

1. 选择 Diagnostics（诊断）> Ping Host（Ping 主机）。打开 Ping Host（Ping 主机）页。



2. 在 IP Address/Host Name（IP 地址/主机名）字段里输入主机名或 IP 地址。

   注意：主机名长度不能超过 232 个字符。

3. 单击 Ping。Result（结果）字段显示 ping 结果。

注意：同时支持 IPv4 地址和 IPv6 地址。

跟踪主机路由页

跟踪路由是网络工具，用于确定至指定主机名或 IP 地址的路由。

▶ 跟踪主机路由：

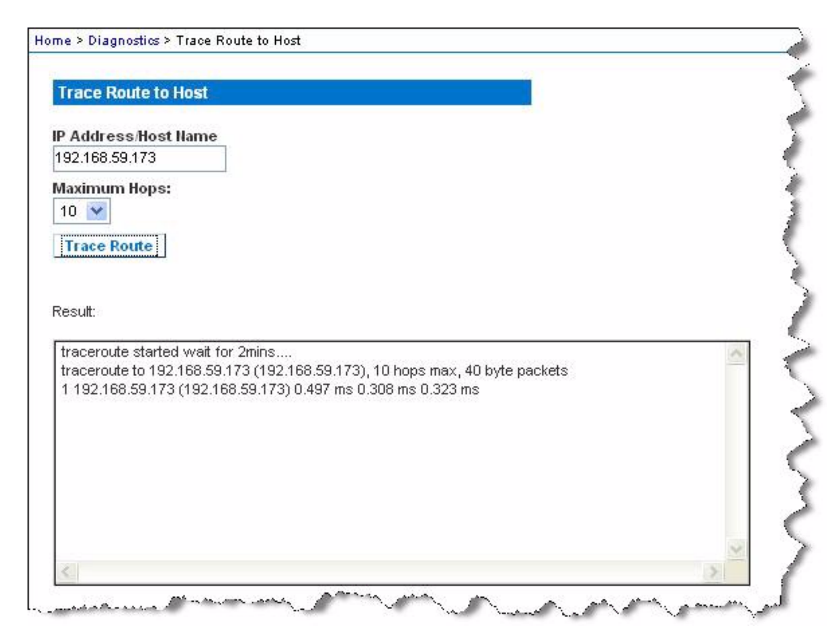
1. 选择 Diagnostics（诊断）> Trace Route to Host（跟踪主机路由）。打开 Trace Route to Host（跟踪主机路由）页。

2. 在 IP Address/Host Name（IP 地址/主机名）字段里输入 IP 地址或主机名。

注意：主机名长度不能超过 232 个字符。

3. 在 Maximum Hops（最大跳数）下拉列表上选择最大跳数（5-50，依次递增 5）。

4. 单击 Trace Route（跟踪路由）。针对指定的主机名或 IP 地址和最大跳数执行跟踪路由命令。Result（结果）字段显示跟踪路由的输出。





设备诊断

注意：本页供 Raritan 现场工程师使用，也可供你在 Raritan 技术支持人员的指导下使用。

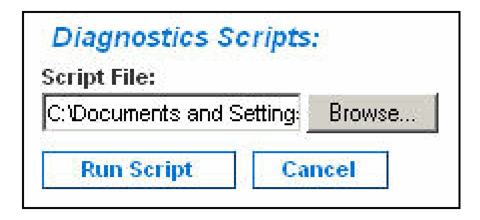
设备诊断功能将 Dominion KX II 上的诊断信息下载到客户机上。可以在本页上执行两个操作：

- 在严重错误调试会话中执行 Raritan 技术支持部门提供的专用诊断脚本。脚本被上载到设备上执行。在执行此脚本之后，可以按 Save to File（保存到文件）按钮下载诊断消息。
- 将 Dominion KX II 设备诊断消息截屏对应的设备诊断日志下载到客户机上。然后将此加密文件发送给 Raritan 技术支持部门。只有 Raritan 能阅读此文件。

注意：只有具备管理权限的用户能访问本页。

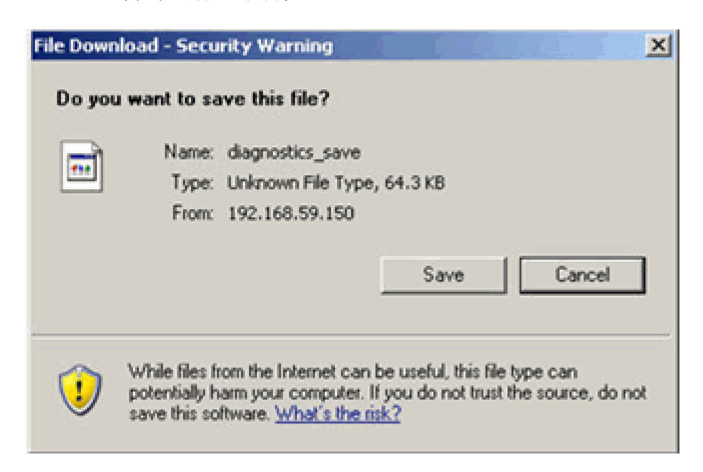
▶ 运行 Dominion KX II 系统诊断：

1. 选择 Diagnostics（诊断）> Dominion KX II Diagnostics（Dominion KX II 诊断）。打开 Dominion KX II Diagnostics（Dominion KX II 诊断）页。
2. 执行 Raritan 技术支持部门通过电子邮件发给你的诊断脚本文件：
   a. 接受并解压（必要时）Raritan 提供的诊断文件。
   b. 单击 Browse（浏览）按钮。打开 Choose File（选择文件）对话框。
   c. 找到并选择诊断文件。
   d. 单击 Open（打开）按钮。Script File（脚本文件）字段显示该文件。



   e. 单击 Run Script（运行脚本）。将此文件发送给 Raritan 技术支持部门。
3. 创建要发送给 Raritan 技术支持部门的诊断文件：

a. 单击 Save to File（保存到文件）按钮。打开 File Download（文件下载）对话框。



b. 单击 Save（保存）按钮。打开 Save As（另存为）对话框。

c. 找到希望的目录，单击 Save（保存）按钮。

d. 按 Raritan 技术支持部门的指示，通过电子邮件发送此文件。



Ch 12 命令行界面

在本章内

概述

假如你有适当的权限，可以用命令行界面配置 Dominion KX II 网络接口，执行诊断功能。

下图概述命令行界面命令。参看***命令行界面命令*** (p. 231)了解所有命令清单，包括命令定义和本章各节的链接，相应的各节举例说明这些命令。

CLI Command Overview

Configuration

Configuring a Network

Connect Commands

Inteface Command

Name Command

可以在上图中的各级命令行界面上使用下列常用命令：top、history、log off、quit、show 和 help。

注意：同时支持 IPv4 地址和 IPv6 地址。

用命令行界面访问 Dominion KX II

用下列方法之一访问 Dominion KX II：

- 基于 IP 连接的 Telnet
- 基于 IP 连接的 SSH (Secure Shell)
- 基于 RS-232 串行接口的本地端口

可以使用多种 SSH/Telnet 客户机，这些客户机可以在下列网站上下载：

- Putty — ***http://www.chiark.greenend.org.uk/~sgtatham/putty/ http://www.chiark.greenend.org.uk/~sgtatham/putty/***
- ssh.com 推出的 SSH Client — ***www.ssh.com http://www.ssh.com***
- Applet SSH Client — ***www.netspace.org/ssh http://www.netspace.org/ssh***
- OpenSSH Client — ***www.openssh.org http://www.openssh.org***

用 SSH 连接访问 Dominion KX II

用支持 SSHv2 的任何 SSH 客户机连接 Dominion KX II。必须在 Devices Services（设备服务）页上启用 SSH 访问。

注意：出于安全原因，Dominion KX II 不支持 SSH V1 连接。

在 Windows PC 上进行 SSH 访问

在 Windows® PC 上启动 SSH 会话：

1. 启动 SSH 客户机软件。
2. 输入 Dominion KX II 服务器的 IP 地址，例如 192.168.0.192。
3. 选择 SSH，它使用默认配置端口 22。
4. 单击 Open（打开）按钮。

显示 `login as:` 提示符。

参看***登录*** (p. 228)。

注意：同时支持 IPv4 地址和 IPv6 地址。



在 UNIX/Linux 工作站上进行 SSH 访问

▶ **如要在 UNIX®/Linux® 工作站上启动 SSH 会话，用 admin 用户名登录，输入下列命令：**

```
ssh -l admin 192.168.30.222
```

显示 Password 提示符。

参看*登录* (p. 228)。

注意：同时支持 IPv4 地址和 IPv6 地址。

用 Telnet 连接访问 Dominion KX II

由于缺乏安全保护，采用明文方式发送用户名、密码和所有流量。默认禁用 Telnet 访问。

启用 Telnet

如果要用 Telnet 访问 Dominion KX II，必须先在命令行界面或浏览器上访问 Dominion KX II。

▶ **启用 Telnet：**

- 在 Device Settings（设备设置）> Device Services（设备服务）菜单上启用 Telnet 访问。

在启用 Telnet 访问之后，可以用它访问 Dominion KX II 并设置其他参数。

在 Windows PC 上进行 Telnet 访问

▶ **在 Windows® PC 上启动 Telnet 会话：**

1. 选择 Startup（启用）> Run（运行）。
2. 在 Open（打开）文本字段里输入 *Telnet*。
3. 单击 OK（确定）按钮。打开 Telnet 页。
4. 在提示符后面输入下列命令：`Microsoft Telnet> open <IP address>`，其中 <IP address> 是 Dominion KX II 的 IP 地址。
5. 按 Enter 键。显示下列消息：显示 `Connecting To <IP address>...The login as` 提示符。

参看*登录* (p. 228)。

注意：同时支持 IPv4 地址和 IPv6 地址。

登录

如要登录，如下输入用户名 admin：

1. 作为 admin 登录
2. 显示 Password 提示符。输入默认密码：*raritan*

   显示欢迎消息。你现在作为管理员登录了。

首先阅读下面的***命令行界面导航*** (p. 229)一节，然后执行初始配置任务。

```
192.168.59.173 - PuTTY
login as: admin
admin@192.168.59.173's password:

------------------------------------------------------------------------------
Device Type:  Dominion KX2       Model: DKX2-232
Device Name:  Dennis_KX2         FW Version: 2.0.20.5.6926       SN: HKB7500230
IP Address:   192.168.59.173     Idle Timeout: 0min
------------------------------------------------------------------------------

Port Port                                  Port          Port   Port
No.  Name                                  Type          Status Availability
2  - Dominion-KX2_Port2                    Not Available down   idle
3  - Dominion_KX2_Port3                    Not Available down   idle
4  - Dominion_KX2_Port4                    Not Available down   idle
5  - Dominion_KX2_Port5                    Not Available down   idle
6  - Dominion_KX2_Port6                    Not Available down   idle
7  - Dominion_KX2_Port7                    Not Available down   idle
8  - P2CIM-AUSB01234567890123456789O1      Not Available down   idle
9  - Dominion_KX2_Port9                    Not Available down   idle
10 - Dominion_KX2_Port10                   Not Available down   idle
11 - Dominion_KX2_Port11                   Not Available down   idle
12 - Dominion_KX2_Port12                   Not Available down   idle
13 - Dominion_KX2_Port13                   Not Available down   idle
14 - Dominion_KX2_Port14                   Not Available down   idle
15 - Dominion_KX2_Port15                   Not Available down   idle
16 - Dominion_KX2_Port16                   Not Available down   idle
17 - Dominion_KX2_Port17                   Not Available down   idle
18 - Dominion_KX2_Port18                   Not Available down   idle
19 - Dominion_KX2_Port19                   Not Available down   idle
20 - Dominion_KX2_Port20                   Not Available down   idle
21 - Dominion_KX2_Port21                   Not Available down   idle
22 - Dominion_KX2_Port22                   Not Available down   idle
23 - Dominion_KX2_Port23                   Not Available down   idle
24 - Dominion_KX2_Port24                   Not Available down   idle
25 - Dominion_KX2_Port25                   Not Available down   idle
26 - Dominion_KX2_Port26                   Not Available down   idle
27 - Dominion_KX2_Port27                   Not Available down   idle
28 - Dominion_KX2_Port28                   Not Available down   idle
29 - Dominion_KX2_Port29                   Not Available down   idle
30 - Dominion_KX2_Port30                   Not Available down   idle
31 - Dominion_KX2_Port31                   Not Available down   idle
32 - Dominion_KX2_Port32                   Not Available down   idle

Current Time: Tue Jun 17 16:27:30 2008
```




命令行界面导航

在使用命令行界面之前，必须了解命令行界面导航和语法。还有一些组合键可以简化命令行界面的使用。

自动完成命令输入

命令行界面支持自动完成部分输入的命令。在输入命令的前面几个字符之后，按 Tab 键。如果这些字符形成唯一匹配，命令行界面自动完成命令输入。

- 如果找不到匹配项，命令行界面显示该级对应的有效输入。
- 如果找到多个匹配项，命令行界面显示所有有效输入。

输入其余字符使输入变成唯一的，按 Tab 键完成命令输入。

命令行界面语法 — 提示和快捷键

提示

- 按字母顺序列出命令。
- 命令不区分大小写。
- 参数名称是一个单词，没有下划线。
- 没有自变量的命令默认显示命令的当前设置。
- 在命令后面输入问号 (?)，显示命令帮助。
- 管道符 (|) 表示在一组可选或必要的关键字或自变量中进行选择。

快捷键

- 按 Up 箭头键显示最后输入的命令。
- 按 Backspace 删除最后输入的字符。
- 按 Ctrl+C 终止命令，或者取消参数输入错误的命令。
- 按 Enter 执行命令。
- 按 Tab 完成命令输入。例如输入 `Admin Port > Conf`，系统显示 `Admin Port > Config >` 提示符。

在命令行界面上常用的命令

下列命令可以在所有命令行界面上执行。这些命令还有助于导航命令行界面。

命令	说明
top	返回命令行界面级联结构的最高层，即 username 提示符。



命令	说明
history	显示用户在 Dominion KX II 命令行界面上输入的最后 200 个命令。
help	显示命令行界面语法概述。
quit	让用户返回第一级。
logout	注销用户会话。

用命令行界面进行初始配置

*注意：命令行界面使用步骤是可选的，因为可以在 KVM 上进行相同的配置。参看*入门 *(p. 14) 了解详情。*

Dominion KX II 设备出厂时有默认出厂设置。在首次通电并连接设备时，必须设置下列基本参数，才能通过网络安全访问设备：

1. 更改管理员密码。所有 Dominion KX II 设备有相同的默认密码。因此，为了避免违反安全要求，必须将管理员密码从 raritan 更改为负责管理 Dominion KX II 设备的管理员的定制密码。
2. 指定 IP 地址、子网掩码和网关 IP 地址，从而启用远程访问。

注意：同时支持 IPv4 地址和 IPv6 地址。

设置参数

为了设置参数，必须登录设备获得管理权限。最高级显示 `Username>` 提示符，初始配置是 `admin`。输入 top 命令，返回最高级菜单。

注意：如果用不同的用户名登录，将显示该用户名，而不显示 admin。

设置网络参数

用 interface 命令配置网络参数。

```
admin > Config > Network > interface enable true if lan1
ip 192.16.151.12 mask 255.255.255 gw 192.168.51.12
```

如果命令被接受，设备自动断开连接。必须使用新 IP 地址和在复位出厂前默认密码部分输入的用户名和密码，重新连接设备。

重要说明：如果忘记了密码，必须按 Dominion KX II 背板上的 Reset（复位）按钮，将 Dominion KX II 复位到出厂前默认设置。如果复位到出厂前默认设置，必须再次执行初始配置。



Dominion KX II 现在有了基本配置，可以通过 SSH 和 GUI 远程访问它，也可以通过本地串行端口访问它。管理员必须配置用户、用户组、服务和安全，以及串行目标服务器连接 Dominion KX II 所用的端口。

注意：同时支持 IPv4 地址和 IPv6 地址。

命令行界面提示符

命令行界面提示符表示当前命令级。提示符的根部分是登录名。对于使用端口仿真应用程序的直接 admin 串行端口连接，Admin Port 是命令的根部分。

```
admin>
```

对于 TELNET/SSH，admin 是命令的根部分：

```
admin > config > network >
```

0

命令行界面命令

- 输入 admin > help。

命令	说明
config	切换到 config 子菜单。
diagnostics	切换到 diag 子菜单。
help	显示命令概述。
history	显示当前会话的命令行历史记录。
listports	列出可访问的端口。
logout	注销当前命令行界面会话。
top	返回根菜单。
userlist	列出活动用户会话。



- 输入 admin > config > network。

命令	说明
help	显示命令概述。
history	显示当前会话的命令行历史记录。
interface	设置/获取网络参数。
ipv6_interface	设置/获取 IPv6 网络参数。
logout	注销当前命令行界面会话。
name	设备名称配置。
quit	返回上一个菜单。
stop	返回根菜单。

安全问题

在解决控制台服务器的安全问题时要考虑的因素：

- 加密在操作员控制台和 Dominion KX II 设备之间发送的数据流量。
- 提供用户验证和授权。
- 安全配置文件。

Dominion KX II 支持所有这些要素，但必须在使用之前进行配置。

管理 Dominion KX II 控制台服务器配置命令

注意：SSH、Telnet 和本地端口访问会话的命令行界面命令相同。

Network 命令可以在 Dominion KX II 的 Configuration（配置）菜单上访问。

配置网络

网络菜单命令用于配置 Dominion KX II 网络适配器。

命令	说明
interface	配置 Dominion KX II 设备网络接口。
name	网络名称配置。



命令	说明
ipv6	设置/获取 IPv6 网络参数。

Interface 命令

Interface 命令用于配置 Dominion KX II 网络接口。interface 命令语法如下：

```
interface [ipauto <none|dhcp>] [ip <ipaddress>] [mask
<subnetmask>] [gw <ipaddress>] [mode <mode>]

Set/Get ethernet parameters

ipauto <none|dhcp> IP auto configuration (none/dhcp)

ip <ipaddress> IP Address

mask <subnetmask> Subnet Mask

gw <ipaddress> Gateway IP Address

mode <mode> Set Ehternet Mode
(auto/10hdx/10fdx/100hdx/100fdx/1000fdx)
```

Interface 命令示例

下列命令启用接口 1，设置 IP 地址、子网掩码和网关地址，将 mode 设置为自动检测。

```
Admin > Config > Network > interface ipauto none ip
192.16.151.12 mask 255.255.255.0 gw 192.168.51.12 mode
auto
```

注意：同时支持 IPv4 地址和 IPv6 地址。



Name 命令

name 命令用于配置网络名称。name 命令语法如下：

```
name [devicename <devicename>] [hostname <hostname>]
```

设备名称配置

```
devicename <devicename>   Device Name
hostname   <hostname>     Preferred host name (DHCP
only)
```

name 命令示例

下列命令设置网络名称：

```
Admin > Config > Network > name devicename My-KSX2
```

IPv6 命令

用 IPv6 命令设置 IPv6 网络参数，获取现有的 IPv6 参数。



Ch 13 Dominion KX II Local Console

在本章内

概述

Dominion KX II 通过本地端口提供机架访问和管理，它的浏览器图形用户界面便于你迅速便捷地在不同的服务器之间来回切换。Dominion KX II Local Console 提供一个直接模拟连接来连接相连的服务器，其性能犹如你直接连接服务器键盘端口、鼠标端口和视频端口。Dominion KX II Local Console 具备与 Dominion KX II Remote Console 相同的管理功能。

使用 Dominion KX II Local Console

并发用户

Dominion KX II Local Console 提供一个独立访问路径，可以访问相连的 KVM 目标服务器。在使用本地控制台时，并不妨碍其他用户同时通过网络连接目标服务器。即使远程用户连接了 Dominion KX II，你也可以在机架上同时通过本地控制台访问服务器。



Dominion KX II Local Console 界面

在服务器机架上进行访问时，Dominion KX II 通过 Dominion KX II Local Console 提供标准 KVM 管理。Dominion KX II Local Console 提供一个直接 KVM（模拟）连接来连接相连的服务器，其性能犹如你直接连接服务器键盘端口、鼠标端口和视频端口。

Dominion KX II Local Console 图形用户界面和 Dominion KX II Remote Console 图形用户界面有许多相似之处。凡是有差异的地方，本帮助都加以说明。

Dominion KX II Local Console 有 Dominion KX II Local Console Factory Reset（出厂复位）选项，但 Dominion KX II Remote Console 没有此选项。

安全和验证

为了使用 Dominion KX II Local Console，必须先用有效用户名和密码进行验证。无论访问是通过网络还是本地端口进行的，Dominion KX II 均具备全集成验证和安全模式。无论在哪种情况下，Dominion KX II 都只允许用户访问那些他们有权访问的服务器。参看***用户管理*** (p. 106)，进一步了解如何指定服务器访问权和安全设置。

如果给 Dominion KX II 配置了外部验证服务（LDAP/LDAPS、RADIUS 或 Active Directory），在本地控制台上进行的验证尝试也通过外部验证服务进行验证。

注意：也可以不给本地控制台访问指定验证；建议你只有在安全环境下才使用此选项。

- **使用 Dominion KX II Local Console：**

1. 把键盘、鼠标和监视器连接到 Dominion KX II 背板上的本地端口。
2. 启动 Dominion KX II。显示 Dominion KX II Local Console 界面。



本地控制台智能卡访问

为了在 Local Console 上用智能卡访问服务器，必须使用 Dominion KX II 的一个 USB 端口，把 USB 智能卡读卡器插入 Dominion KX II。在 Dominion KX II 上插入或拔下智能卡读卡器之后，Dominion KX II 自动监测读卡器。参看***支持的和不支持的智能卡读卡器*** (p. 270)和***最低系统要求*** (p. 272)，了解支持的智能卡和其他系统要求清单。

在目标服务器上安装读卡器之后，可以像使用直接连接的读卡器一样使用服务器上的读卡器和智能卡。在取下智能卡或智能卡读卡器之后，根据在目标服务器操作系统上设置的取卡策略，系统要么锁定用户会话，要么不让你退出系统。在因关闭 KVM 会话或切换到新目标服务器而终止 KVM 会话之后，自动把智能卡读卡器从目标服务器上卸载掉。

► **通过 Dominion KX II Local console 把智能卡读卡器安装在目标服务器上：**

1. 使用 Dominion KX II 的一个 USB 端口，把 USB 智能卡读卡器插入此设备。在连接智能卡读卡器之后，Dominion KX II 检测读卡器。
2. 单击 Local Console 上的 Tools（工具）。
3. 在 Card Readers Detected（检测到的读卡器）列表上选择智能卡读卡器。如果不想安装智能卡读卡器，选择 None（无）。
4. 单击 OK（确定）按钮。在添加智能卡读卡器之后，页面显示一条消息，说明你成功完成了操作。在页面左面板上的 Card Reader（读卡器）下面，显示 Selected（已选择）或 Not Selected（未选择）状态。

▶ 更新检测到的读卡器列表：

- 如果安装了新智能卡，单击 Refresh（刷新）按钮。刷新 Card Readers Detected（检测到的读卡器）列表，反映新添加的智能卡读卡器。

Select Card Reader

Card Readers Detected

None
USB SmartCard Reader (Gemplus)



在 KX2 8 设备上进行智能卡访问

如果在 Local Console 上使用智能卡读卡器，通过 KX2-832 或 KX2-864 设备访问服务器，必须禁用扩展本地端口（Local Port Settings[本地端口设置]页）。扩展本地端口不支持智能卡验证。

本地控制台 USB 配置文件选项

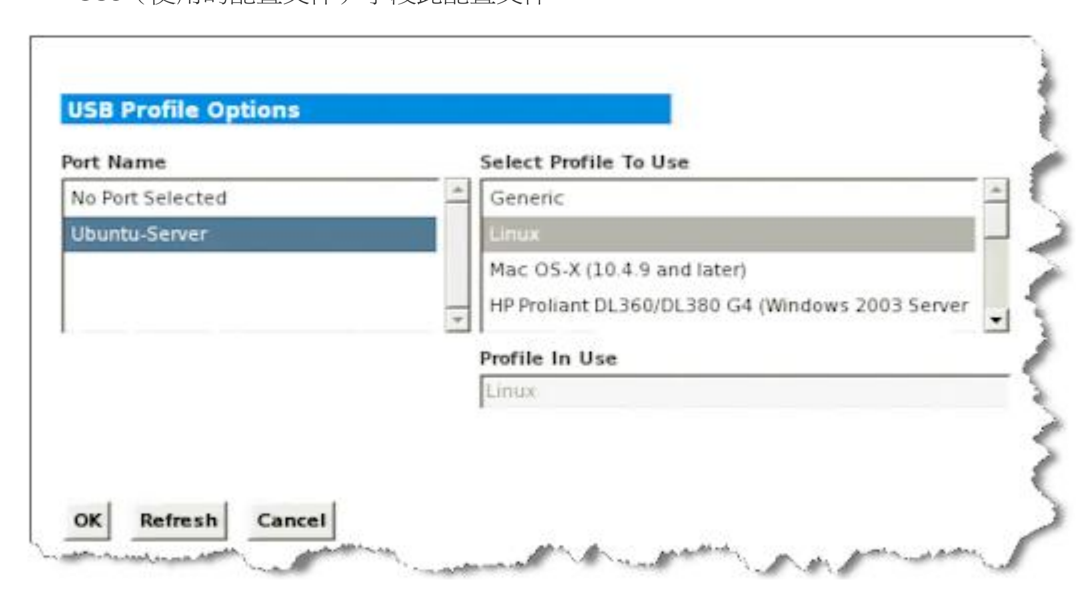
在 Tools（工具）页的 USB Profile Options（USB 配置文件选项）部分给本地端口选择可用的 USB 配置文件。

Port Name（端口名称）字段显示可以指定配置文件的端口，在选择端口之后，Select Profile To Use（选择要使用的配置文件）字段显示可供此端口使用的配置文件。Profile In Use（使用的配置文件）字段显示给端口选择的配置文件。

▶ 将 USB 配置文件应用于本地控制台端口：

1. 在 Port Name（端口名称）字段里选择要把 USB 配置文件应用于哪个端口。

2. 在 Select Profile to Use（选择要使用的配置文件）字段里给端口选择要使用的配置文件。
3. 单击 OK（确定）按钮。把 USB 配置文件应用于本地端口，Profile In Use（使用的配置文件）字段此配置文件。



可用分辨率

Dominion KX II Local Console 提供下列分辨率支持各种监视器：

- 800x600
- 1024x768
- 1280x1024

每种分辨率的刷新率有两个：60Hz 和 75Hz。

端口访问页（本地控制台服务器显示器）

在登录 Dominion KX II Local Console 之后，打开 Port Access（端口访问)页。本页列出所有 Dominion KX II 端口、相连的 KVM 目标服务器、及其状态和可用性。

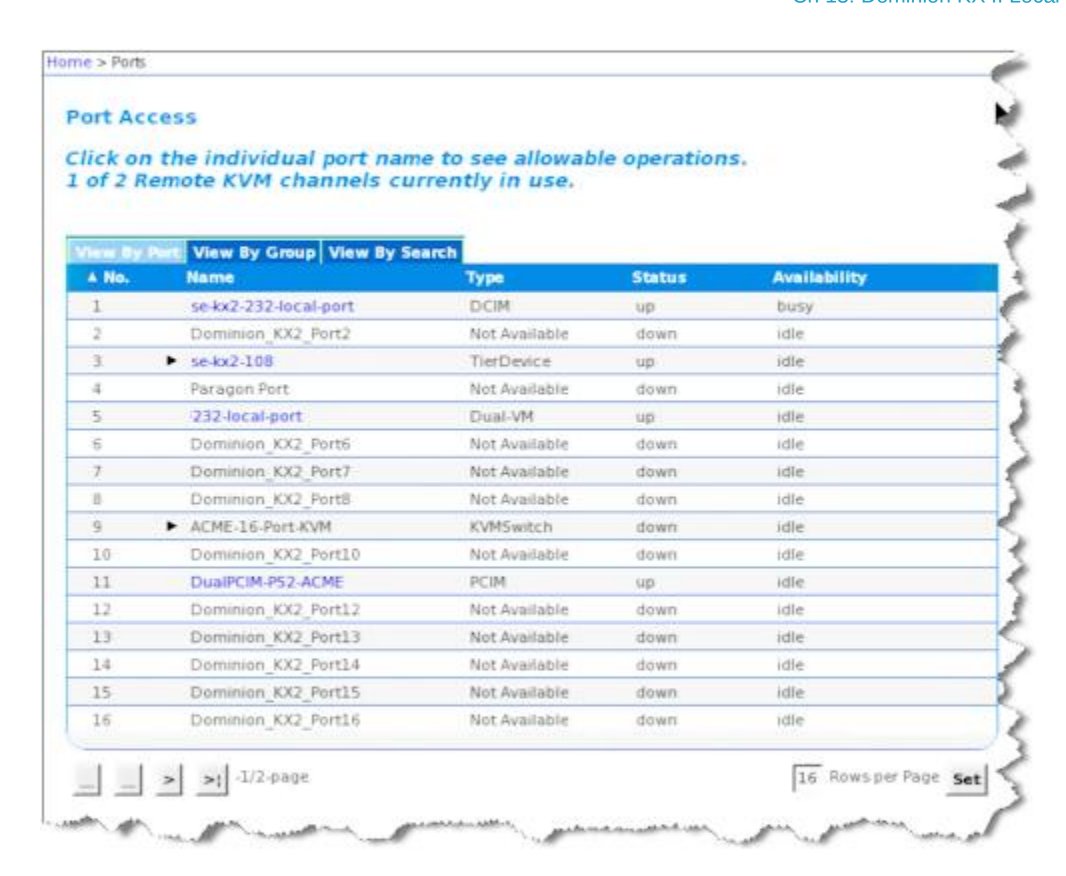
Port Access（端口访问）页还显示在 Dominion KX II 上配置的刀片服务器机箱。Port Access（端口访问）页采用可展开的分层形式显示刀片服务器机箱，刀片服务器机箱位于分层结构的根部，根下面显示各个有标号的刀片服务器。单击根机箱旁边的展开箭头图标显示各个刀片服务器。

注意：如要按分层顺序查看刀片服务器机箱，必须给刀片服务器机箱配置刀片服务器机箱子类型。

如果使用级联配置，用基础 Dominion KX II 设备访问多台其他级联设备，单击基础设备名称左边的展开箭头图标 ，在 Port Access（端口访问）页上查看级联设备。 如果使用级联配置，用基础 Dominion KX II 设备访问多台其他级联设备，单击基础设备名称左边的展开箭头图标 ►，在 Port Access（端口访问）页上查看级联设备。 参看***配置和启用级联*** (p. 137) 详细了解级联。

Port Access（端口访问）页默认显示 View by Port（按端口查看）选项卡。View by Group（按组查看）选项卡显示端口组，可以展开显示给此端口组指定的端口。 View by Search（按搜索结果查看）选项卡允许你按端口名称进行搜索。搜索功能支持星号 (*) 通配符、全名和部分名称。





▶ **使用端口访问页：**

1. 登录 Local Console。

   KVM 目标服务器最初按 Port Number（端口号）排序。可以更改显示方式，按任何一列排序。

   - Port Number（端口号）— 从 1 到 Dominion KX II 设备的总端口数进行编号。注意这里不列出与电源条相连的端口，导致 Port Number（端口号）序列不连续。
   - Port Name（端口名称）— Dominion KX II 端口的名称。端口名称最初设置为 Dominion-KX2-Port#，但可以将名称更改为更具说明性的名称。在单击 Port Name（端口名称）链接时，打开 Port Action（端口操作）菜单。

   注意：切勿在 Port (CIM) Name（端口 (CIM) 名称）中使用撇号。

   - Status（状态）— 目标服务器的标准状态是工作或停止。
   - Type（类型）— 服务器或 CIM 的类型。对于刀片服务器机箱，类型可以是 Blade Chassis（刀片服务器机箱）、Blade（刀片服务器）、BladeChassisAdmin 和 BladeChassisURL。类型还包括级联的设备和 KVM 交换机。



- Availability（可用性）— 可用性可以是 Idle（空闲）、Connected（已连接）、Busy（忙）或 Unavailable（不可用）。当刀片服务器连接工作时，刀片服务器的可用性可以是 shared（共享）或 exclusive（独占）。

2. 单击 View by Port（按端口查看）或 View by Group（按组查看），在不同的视图之间来回切换。
   - 除了 Port Number（端口号）、Port Name（端口名称）、Status（状态）、Type（类型）和 Availability（可用性），View by Group（按组查看）选项卡还显示 Group（组）列。本列包含可用的端口组。
3. 单击要访问的目标服务器的 Port Name（端口名称）。打开 Port Action（端口操作）菜单。参看**端口操作菜单** (p. 43)详细了解可用菜单项。
4. 在 Port Action（端口操作）菜单上选择期望的菜单命令。

▶ 更改显示排序顺序：

- 单击要按哪一列排序。按该列排序 KVM 目标服务器列表。

热键和连接键

由于 Dominion KX II Local Console 界面被你访问的目标服务器的界面取代了，所以用热键断开目标服务器，返回本地端口 GUI。用连接键连接目标服务器，在多台目标服务器之间来回切换。

在显示目标服务器时，可以用本地端口热键迅速返回 Dominion KX II Local Console 用户界面。默认设置是迅速按两次 Scroll Lock 键，但你可以（在 Local Port Settings [本地端口设置]页上）指定另一个组合键作为热键。参看 Dominion KX II Local Console 本地端口设置了解详情。

连接键示例

标准服务器	
连接键操作	**热键示例**
在本地端口 GUI 上访问端口	在本地端口 GUI 上访问端口 5： • 按住左 ALT > 按 5 > 释放左 ALT
切换端口	从目标服务器端口 5 切换到端口 11： • 按住左 ALT > 按 1 > 按 1 > 释放左 ALT
断开目标服务器，返回本地端口 GUI	断开目标服务器端口 11，返回本地端口 GUI（连接目标服务器所用的页面）：



标准服务器	
连接键操作	**热键示例**
	• 双击 Scroll Lock

刀片服务器机箱	
连接键操作	**热键示例**
在本地端口 GUI 上访问端口	访问端口 5、插槽 2： • 按住左 ALT > 按 5 > 按 - > 按 2 > 释放左 ALT
切换端口	从目标服务器端口 5、插槽 2 切换到端口 5、插槽 11： • 按住左 ALT > 按 5 > 按 - > 按 1 > 按 1 > 释放左 ALT
断开目标服务器，返回本地端口 GUI	断开目标服务器端口 5、插槽 11，返回本地端口 GUI（连接目标服务器所用的页面）： • 双击 Scroll Lock

Sun 特殊组合键

在本地端口上使用下列 Sun Microsystems 服务器特殊组合键。在连接 Sun™ 目标服务器之后，可以在 Keyboard（键盘）菜单上访问这些特殊组合键：

Sun 键	本地端口组合键
Again	Ctrl+ Alt +F2
Props	Ctrl + Alt +F3
Undo	Ctrl + Alt +F4
Stop A	Break a
Front	Ctrl + Alt + F5
Copy	Ctrl + Alt + F6
Open	Ctrl + Alt + F7
Find	Ctrl + Alt + F9
Cut	Ctrl + Alt + F10



Sun 键	本地端口组合键
Paste	Ctrl + Alt + F8
Mute	Ctrl + Alt + F12
Compose	Ctrl+ Alt + KPAD *
Vol +	Ctrl + Alt + KPAD +
Vol -	Ctrl + Alt + KPAD -
Stop	没有组合键
Power	没有组合键

访问目标服务器

▶ 访问目标服务器：

1. 单击要访问的目标服务器的 Port Name（端口名称）。显示 Port Action（端口操作）菜单。
2. 在 Port Action（端口操作）菜单上选择 Connect（连接）。监视器切换到目标服务器界面。

返回 Dominion KX II Local Console 界面

重要说明：Dominion KX II Local Console 默认热键是迅速按两次 Scroll Lock 键。可以在 Local Port Settings（本地端口设置）页上更改此组合键。参看 Dominion KX II Local Console 本地端口设置。

▶ 从目标服务器返回 Dominion KX II Local Console：

- 迅速按两次热键（默认热键是 Scroll Lock）。监视器从目标服务器界面切换到 Dominion KX II Local Console 界面。



本地端口管理

Dominion KX II 既可以用 Dominion KX II Local Console 管理，也可以用 Dominion KX II Remote Console 管理。注意 Dominion KX II Local Console 还提供下列访问：

- 出厂复位
- 本地端口设置（也可以在远程控制台上使用）

注意：只有具有管理权限的用户能访问这些功能。

配置 Dominion KX II Local Console 本地端口设置

可以在 Local Port Settings（本地端口设置）页上定制 Dominion KX II Local Console 的许多设置，包括键盘、热键、视频切换延迟、节电模式、本地用户界面分辨率设置和本地用户验证。

注意：只有具有管理权限的用户能访问这些功能。

▶ 配置本地端口设置：

注意：在 Local Port Settings（本地端口设置）页上更改某些设置之后，要重新启动正在使用的浏览器。如果在更改设置时重新启动浏览器，将记录设置步骤。

1. 选择 Device Settings（设备设置）> Local Port Settings（本地端口设置）。打开 Local Port Settings（本地端口设置）页。
2. 在键盘类型下拉列表上的选项中选择合适的键盘类型。在进行更改时，重新启动浏览器。
   - US（美国英语）
   - US/International（美国英文/国际）
   - United Kingdom（英国英语）
   - French (France)（法文[法国]）
   - German (Germany)（德文[德国]）
   - JIS（日本工业标准）
   - Simplified Chinese（简体中文）
   - Traditional Chinese（繁体中文）
   - Dubeolsik Hangul（朝鲜文）
   - German (Switzerland)（德文[瑞士]）



- Portuguese（葡萄牙）
- Norwegian (Norway)（挪威文[挪威]）
- Swedish (Sweden)（瑞典文[瑞典]）
- Danish (Denmark)（丹麦文[丹麦]）
- Belgian (Belgium)（比利时）

注意：中文键盘、日文键盘和朝鲜文键盘仅用于显示。Dominion KX II Local Console 功能目前不支持本地语言输入。

3. 选择本地端口热键。在显示目标服务器界面时，可以用本地端口热键返回 Dominion KX II Local Console 界面。默认设置是按双击 Scroll Lock，但可以在下拉列表上选择任何组合键：

热键：	执行此操作：
双击 Scroll Lock	迅速按两次 Scroll Lock 键
双击 Num Lock	迅速按两次 Num Lock 键
双击 Caps Lock	迅速按两次 Caps Lock 键
双击左 Alt 键	迅速按两次左 Alt 键
双击左 Shift 键	迅速按两次左 Shift 键
双击左 Ctrl 键	迅速按两次左 Ctrl 键

4. 选择 Local Port Connect key（本地端口连接键）。用连接键连接目标服务器，切换到另一台目标服务器。可以用热键断开目标服务器，返回本地端口 GUI。连接键适用于标准服务器和刀片服务器机箱。在创建本地端口连接键之后，GUI 导航面板显示该键，所以你可以用它作为参考。参看***连接键示例*** (p. 242)了解连接键顺序示例。
5. 必要时将 Video Switching Delay（视频切换延迟）设置为 0-5 秒。通常使用 0，除非需要更长的时间（某些监视器要求的视频切换时间较长）。
6. 如果要使用节电功能：
   a. 选择 Power Save Mode（节电模式）复选框。
   b. 设置在启动节电模式之前经过的时间（分钟）。
7. 在 Resolution（分辨率）下拉列表上选择 Dominion KX II Local Console 的分辨率。在进行更改时，重新启动浏览器。
   - 800x600
   - 1024x768
   - 1280x1024

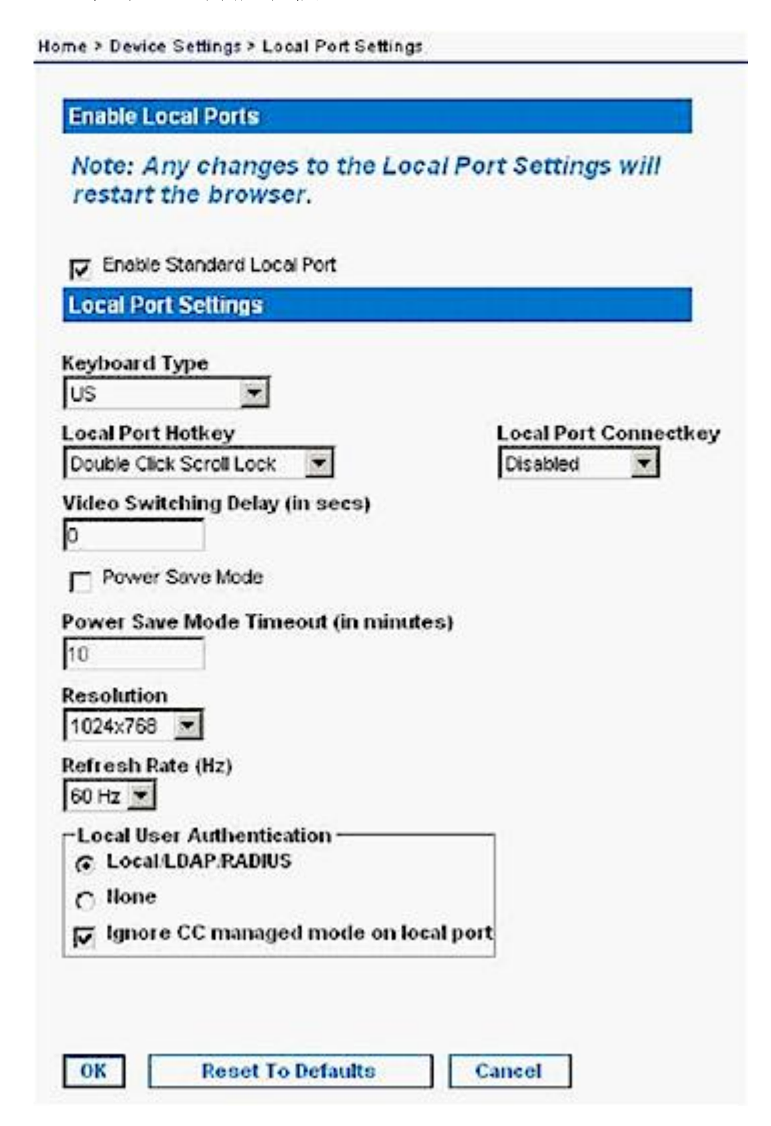


8. 在 Refresh rate（刷新速率）下拉列表上选择刷新速率。 在进行更改时，重新启动浏览器。
   - 60 Hz
   - 75 Hz
9. 选择本地用户验证类型。
   - Local/LDAP/RADIUS。这是建议的选项。参看***远程验证*** (p. 34)进一步了解验证。
   - 不用安装任何软件。本地控制台访问不使用验证。建议你只在安全环境下使用此选项。
   - 如果希望本地用户在 Dominion KX II 受 CC-SG 管理的情况下也访问它，选择 Ignore CC managed mode on local port（在本地端口忽略 CC 管理模式）复选框。

注意：如果最初选择在本地端口不忽略 CC 管理模式，但稍后要进行本地端口访问，必须在 CC-SG 上让设备不再受 CC-SG 管理，然后可以选择此复选框。



10. 单击 OK（确定）按钮。



在 Local Console 上配置 Dominion KX II 本地端口设置

可以在 Remote Console 的 Port Configuration（端口配置）页上或 Local Console 的 Local Port Settings（本地端口设置）页上配置标准本地端口和扩展本地端口。参看***配置 Dominion KX II 本地端口设置*** (p. 185)，详细了解如何配置这些端口。



Dominion KX II Local Console 出厂复位

注意：只能在 Dominion KX II Local Console 上使用此功能。

Dominion KX II 在本地控制台用户界面上提供几种复位方式。

*注意：建议你在执行出厂复位之前保存审计日志。在执行出厂复位时删除审计日志，不在审计日志里记录复位事件。如要进一步了解如何保存审计日志，参看**审计日志**。*

► 执行出厂复位：

1. 选择 Maintenance（维护）> Factory Reset（出厂复位）。打开 Factory Reset（出厂复位）页。
2. 在下列选项中选择合适的复位选项：

- Full Factory Reset（全出厂复位）— 删除整个配置，将设备彻底复位到出厂前默认值。注意：用 CommandCenter 定义的任何管理关联被断开。由于这种复位是全复位，系统提示你确认出厂复位。
- Network Parameter Reset（网络参数复位）— 将设备的网络参数复位到默认值（单击 Device Settings（设备设置）> Network Settings（网络设置）访问这些信息）：
  - IP auto configuration（IP 自动配置）
  - IP address（IP 地址）
  - Subnet mask（子网掩码）
  - Gateway IP address（网关 IP 地址）
  - Primary DNS server IP address（主 DNS 服务器 IP 地址）
  - Secondary DNS server IP address（备用 DNS 服务器 IP 地址）
  - Discovery port（发现端口）
  - Bandwidth limit（带宽极限）
  - LAN interface speed & duplex（LAN 接口速度和双工）
  - Enable automatic failover（启用自动故障切换）
  - Ping interval (seconds)（Ping 间隔[秒]）
  - Timeout (seconds)（超时[秒]）

1. 单击 Reset（复位）按钮继续。由于将永久丢失所有网络设置，系统提示你确认出厂复位。
2. 单击 OK（确定）按钮继续。在复位结束之后，Dominion KX II 设备自动重新启动。



用复位按钮复位 Dominion KX II

设备背板上有 Reset（复位）按钮。此按钮深陷在背板上，防止意外复位（需要用尖物体按此按钮）。

在按 Reset（复位）按钮时执行的操作，要在图形用户界面上定义。参看加密和共享。

注意：建议你在执行出厂复位之前保存审计日志。在执行出厂复位时删除审计日志，不在审计日志里记录复位事件。如要进一步了解如何保存审计日志，参看审计日志。

▶ 复位设备：

1. 断开 Dominion KX II 电源。
2. 使用尖头物按下 Reset（复位）按钮。
3. 继续按住 Reset（复位）按钮，重新接通 Dominion KX II 设备电源。
4. 按住 Reset（复位）按钮 10 秒钟。 在设备复位之后，发出两声短促的蜂鸣声，表示复位结束了。





Ap A 规格

在本章内

物理规格

Dominion KX II 规格

零件编号	项目说明	UPC 代码	电源	重量	产品尺寸 (WxDxH)	包装重量	包装尺寸 (WxDxH)
DKX2-108	8 端口 Dominion KX II，单用户网络访问和本地端口，虚拟媒体，双电源	785813624109	双电源 100/240V 50/60Hz 0.6A 25W	8.58 磅	1.75" x 17.32" x 11.4"	14.3 磅	22" x 16.6" x 6.5"
				3.9 公斤	44mm x 439mm x 290mm	6.5 公斤	559mm x 422mm x 165mm
DKX2-116	16 端口 Dominion KX II，单用户网络访问和本地端口，虚拟媒体，双电源	785813624055	双电源 100/240V 50/60Hz 0.6A 25.4W	8.65 磅	1.75" x 17.3" x 11.4"	14.85 磅	22" x 16.6" x 6.5"
				3.9 公斤	44mm x 439mm x 290mm	6.7 公斤	559mm x 422mm x 165mm



零件编号	项目说明	UPC 代码	电源	重量	产品尺寸 (WxDxH)	包装重量	包装尺寸 (WxDxH)
DKX2-132	32 端口 Dominion KX II，单用户网络访问和本地端口，虚拟媒体，双电源	785813624079	双电源 100/240V 50/60Hz 0.6A 26W	9.0 磅	1.75" x 17.3" x 11.4"	14.9 磅	22" x 16.6" x 6.5"
				4.1 公斤	44mm x 439mm x 290mm	6.8 公斤	559mm x 422mm x 165mm
DKX2-216	16 端口 Dominion KX II，二用户网络访问和本地端口，虚拟媒体，双电源	785813624086	双电源 100/240V 50/60Hz 0.6A 26.3W	8.65 磅	1.75" x 17.3" x 11.4"	14.49 磅	22" x 16.6" x 6.5"
				3.9 公斤	44mm x 439mm x 290mm	6.6 公斤	559mm x 422mm x 165mm
DKX2-232	32 端口 Dominion KX II，二用户网络访问和本地端口，虚拟媒体，双电源	785813625021	双电源 100/240V 50/60Hz(最佳 47-63Hz) 0.6A 27W	9.0 磅	1.75" x 17.3" x 11.4"	14.9 磅	22" x 16.6" x 6.5"
				4.1 公斤	44mm x 439mm x 290mm	6.8 公斤	559mm x 422mm x 165mm
DKX2-416	16 端口 Dominion KX II，四用户网络访问和本地端口，虚拟媒体，双电源	785813625359	双电源 100/240V 50/60Hz 1A 62W	9.04 磅	17.3” x 11.6” x 1.75”	14.94 磅	22” x 16.5” x 6.5”
				4.1 公斤	440 mm x 295 mm x 44 mm	6.8 公斤	560 mm x 420 mm x 165 mm
DKX2-432	32 端口 Dominion KX II，四用户网络访问和本地端口，虚拟媒体，双电源	785813625380	双电源 100/240V 50/60Hz 1A 64W	9.48 磅	17.3” x 11.6” x 1.75”	15.38 磅	22” x 16.5” x 6.5”
				4.3 公斤	440 mm x 295 mm x 44 mm	7.0 公斤	560 mm x 420 mm x 165 mm
DKX2-464	64 端口 Dominion KX II，四用户网络访问和本地端口，虚拟媒体，双电源	785813625298	双电源 100/240V 50/60Hz 1A 64W	11.29 磅	17.3” x 11.6” x 3.5”	19.8 磅	22” x 16.5” x 6.5”
				5.12 公斤	440 mm x 295 mm x 88 mm	9 公斤	560 mm x 420 mm x 165 mm



KX2-8 规格

零件编号	项目说明	UPC 代码	电源	重量	产品尺寸 (WxDxH)	包装重量	包装尺寸 (WxDxH)
DKX2-832	32 端口 Dominion KX II，八用户网络访问，标准本地端口，扩展本地端口，虚拟媒体，双电源	0785813620019	双电源 100/240V 50/60Hz 1A (0.5A) 64W	10.57 磅	17.3” x 14.2” x 1.73”	35.90 磅	22” x 18.5” x 11”
				4.8 公斤	440 mm x 360 mm x 44 mm	16.3 公斤	560 mm x 470 mm x 280 mm
DKX2-864	64 端口 Dominion KX II，八用户网络访问，标准本地端口，扩展本地端口，虚拟媒体，双电源	0785813620026	双电源 100/240V 50/60Hz 1.2A 64W	13.22 磅	17.3” x 14.6” x 3.5”	22.47 磅	21.7” x 20.1” x 7.5”
				6.0 公斤	440 mm x 370 mm x 88 mm	10.2 公斤	550 mm x 510 mm x 190 mm

环境要求

工作时	
温度	0°C- 40°C
湿度	20% - 85% 相对湿度
海拔	不适用
振动	5-55-5 HZ，0.38mm，1 分/周期； 每个轴 (X,Y,Z) 30 分钟
冲击	不适用
不工作时	
温度	0°C-50°C
湿度	10% - 90% 相对湿度
海拔	不适用
振动	5-55-5 HZ，0.38mm，1 分/周期；



工作时	
	每个轴 (X,Y,Z) 30 分钟
冲击	不适用

计算机接口模块 (CIM)

零件编号	项目说明	产品重量	产品尺寸 (WxDxH)	包装重量	包装尺寸 (WxDxH)	UPC 代码
D2CIM-VUSB	Dominion KX II 计算机接口模块 [USB 端口和虚拟媒体]	0.2 磅	1.3" x 3.0" x 0.6"	0.2 磅	7.2" x 9" x 0.6"	785813332004
DCIM-PS2	Dominion KX I 和 II 计算机接口模块 [PS/2 端口]	0.2 磅	1.3" x 3.0" x 0.6"	0.2 磅	7.2" x 9" x 0.6"	785813338532
DCIM-USB	Dominion KX I 和 II 计算机接口模块 [USB 端口]	0.2 磅	1.3" x 3.0" x 0.6"	0.2 磅	7.2" x 9" x 0.6"	785813338518
DCIM-SUSB	Dominion KX I 和 II 计算机接口模块 [Sun USB 端口]	0.2 磅	1.3" x 3.0" x 0.6"	0.2 磅	7.2" x 9" x 0.6"	785813338556
DCIM-USBG2	Dominion KX I 和 II 计算机接口模块 [USB 和 Sun USB 端口] G2 CIM	0.2 磅	1.3" x 3.0" x 0.6"	0.2 磅	7.2” x 9” x 0.6	785813338884
DCIM-SUN	Dominion KX I 和 II 计算机接口模块 [Sun 端口，HD15 视频]	0.2 磅	1.3" x 3.0" x 0.6"	0.2 磅	7.2" x 9" x 0.6"	785813338549
D2CIM-PWR	Dominion KX II 远程电源条计算机接口模块	0.2 磅	1.3" x 3.0" x 0.6"	0.2 磅	7.2" x 9" x 0.6"	785813332011



零件编号	项目说明	产品重量	产品尺寸 (WxDxH)	包装重量	包装尺寸 (WxDxH)	UPC 代码
D2CIM-VUSB-32PAC	32 个 D2CIM-VUSB 散装	6.4 磅	(1.3" x 3.0" x 0.6")*32	8.01 磅	21.65"x 12.20"x 4.33"	785813332028
D2CIM-VUSB -64PAC	64 个 D2CIM-VUSB 散装	12.8 磅	(1.3" x 3.0" x 0.6")*64	18.13 磅	22.64"x 9.45"x 12.99"	785813332035
D2CIM-DVUSB	Dominion KX II 计算机接口模块 [双 USB 端口和虚拟媒体]	0.23 磅，105 克	3.53" x 1.68" x .76" 89.7x42.7x19.3 (mm)	0.25 磅，112.5 克	3.9" x 5.7" x 1.0" 100*145*27 (mm)	785813339508
D2CIM-DVUSB-32PAC	32 个 D2CIM-DVUSB 散装	10.1 磅，4.6 公斤	21.9" x 12.2" x 4.3" 555x310x110 (mm)	10.1 磅，4.6 公斤	21.9" x 12.2" x 4.3" 555x310x110 (mm)	785813332080
D2CIM-DVUSB -64PAC	64 个 D2CIM-DVUSB 散装	22.5 磅，10.2 公斤	9.4" x 22.6" x 13.0" 240x575x330 (mm)	22.5 磅，10.2 公斤	9.4" x 22.6" x 13.0" 240*575*330 (mm)	785813332097

支持的 CIM 和操作系统（目标服务器）

除了新的 Dominion KX II D2CIM，还支持大多数 Paragon® CIM 和 Dominion KX I CIM。下表列出支持的目标服务器操作系统、CIM、虚拟媒体和鼠标模式。

注意：对于第一代设备，只支持 32 位 Windows® 和 Linux® 目标服务器操作系统。



支持的 **Paragon CIM**	操作系统和串行设备（如适用）	虚拟媒体	绝对鼠标模式	智能鼠标模式	标准鼠标模式
• P2CIM-PS2	• Windows XP® • Windows 2000® • Windows 2000 Server® • Windows 2003 Server® • Windows Vista® • Windows 7® • Windows 2008® • Red Hat® Enterprise Linux® 4 ES • Red Hat Enterprise Linux 5 • Open SUSE 10, 11 • Fedora® 8 - 11 • IBM® AIX™ • HP UX			✓	✓
• P2CIM-AUSB • UUSBPD	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Red Hat Enterprise Linux 4 ES • Red Hat Enterprise Linux 5 • Open SUSE 10, 11 • Fedora 8 - 11 • IBM AIX • HP UX • Mac® OS			✓	✓



支持的 **Paragon CIM**	操作系统和串行设备(如适用)	虚拟媒体	绝对鼠标模式	智能鼠标模式	标准鼠标模式
• UKVMPD (version 0C4) *注意:V0C5 不支持 Dominion KX II。*	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Red Hat Enterprise Linux 4 ES • Red Hat Enterprise Linux 5 • Open SUSE 10, 11 • Fedora 8 - 11			✓	✓
• P2CIM-SUN • P2CIM-SUSB	• Dominion KX I 支持所有 Solaris™ 操作系统				✓
• P2CIM-SER	• 串行设备				



支持的 **Dominion KX I DCIM**	目标服务器	虚拟媒体	绝对鼠标模式	智能鼠标模式	标准鼠标模式
• DCIM-PS2	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Red Hat Enterprise Linux 4 ES • Red Hat Enterprise Linux 5 • Open SUSE 10, 11 • Fedora Core 3 和更高版本 • IBM AIX • HP UX			✓	✓
• DCIM-USB	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Red Hat Enterprise Linux 4 ES • Red Hat Enterprise Linux 5 • Open SUSE 10, 11 • Fedora 8 - 11 • Mac OS • IBM AIX • HP UX			✓	✓



支持的 **Dominion KX I DCIM**	目标服务器	虚拟媒体	绝对鼠标模式	智能鼠标模式	标准鼠标模式
• DCIM-USBG2	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Red Hat Enterprise Linux 4 ES • Red Hat Enterprise Linux 5 • Open SUSE 10, 11 • Fedora 8 - 11 • Mac OS • Dominion KX I 支持所有 Solaris 操作系统 • IBM AIX • HP UX			✓	✓
注意：DCIM-USBG2 和 P2CIM-AUSB 在 CIM 背面有一个很小的滑动开关。对于 PC 型 USB 目标服务器，将开关打到 P 位置；对于 Sun USB 目标服务器，将开关打到 S 位置。只有在给 CIM 重新通电之后，新切换器位置才会生效。如要给 CIM 重新通电，取下目标服务器上的 USB 连接器，稍后再插回去几秒钟。					
• DCIM-SUN • DCIM-SUSB	• Dominion KX I 支持所有 Solaris 操作系统			✓	✓

支持的 **Dominion KX II D2CIM**	目标服务器和远程电源条（如适用）	虚拟媒体	绝对鼠标模式	智能鼠标模式	标准鼠标模式
• D2CIM-VUSB	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Open SUSE 10, 11 • Fedora Core 3 和更高版本 • Red Hat Enterprise Linux 4 ES • Red Hat Enterprise Linux 5 • Mac OS	✓	✓*	✓	✓
注意：Sun™ (Solaris) 目标服务器不支持 D2CIM-VUSB。 **Linux 操作系统不支持绝对鼠标模式。*					
• D2CIM-DVUSB	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Open SUSE 10, 11 • Fedora 8 - 11 • Mac OS	✓	✓	✓	✓
• D2CIM-PWR	• 远程电源条				



支持的 Paragon CIM 和配置

Dominion KX II 支持 P2CIM-APS2DUAL 和 P2CIM-AUSBDUAL CIM，提供两个 RJ45 端口连接不同的 KVM 切换器。支持这些 CIM，在其中一台 KVM 切换器被封锁或发生故障时，可以采用这种备用方法访问目标服务器。

Paragon CIM	支持	不支持
P2CIM-SUN	• 配备 IBM® PS/2 型键盘端口和鼠标端口的服务器 • 自动纠偏补偿（当 CIM 连接 Paragon II 而非 Dominion KX II 连接 Paragon 时） • 智能鼠标模式 • 标准鼠标模式	• 虚拟媒体 • 智能卡 • 绝对鼠标模式 • 与刀片服务器机箱一起使用 • 级联 KVM 配置
P2CIM-AUSBDUAL	• 配备 USB 型或 Sun™ USB 型键盘端口和鼠标端口的服务器 • 自动纠偏补偿（当 CIM 连接 Paragon II 而非 Dominion KX II 连接 Paragon 时） • 智能鼠标模式 • 标准鼠标模式	• 虚拟媒体 • 智能卡 • 绝对鼠标模式 • 与刀片服务器机箱一起使用 • 级联 KVM 配置



Dominion KX II 到 Dominion KX II 配置原则

在 Dominion KX II 到 **Dominion KX II** 配置中使用 **Paragon CIM** 时，**应该遵循下列系统配置原则：**

并发访问

并发访问禁止所有用户组同时访问所有目标服务器。

- 应该给两台 Dominion KX II KVM 切换器配置相同的目标服务器并发访问策略。
- 如果需要独占访问目标服务器，必须把两台 KVM 切换器的 PC-Share（PC 共享）模式设置为 Private（独占）。参看***加密和共享*** (p. 193)。

注意：如果在与 Dominion KX II 一起使用 P2CIM-APS2DUAL 或 P2CIM-AUSBDUAL 时必须保证隐私，不要使用用户组 PC 共享权限。

CIM 名称更新

P2CIM-APS2 名称和 P2CIM-AUSB 名称存储在 CIM 的内存里。有两个存储单元，可以满足 Paragon 命名常规（12 个字符）和 Dominion KX II 命名常规（32 个字符）要求。

在首次连接 Dominion KX II 时，在内存里检索 Paragon 名称，把它写入 Dominion KX II 使用的 CIM 存储单元。在后续查询 CIM 名称或更新 Dominion KX II 上的 CIM 名称时，更改 Dominion KX II 使用的存储单元。Dominion KX II 不更新 Paragon II 使用的存储单元。

当一台 Dominion KX II 更新 CIM 名称时，另一台 Dominion KX II 在下次尝试连接目标服务器时检测并检索更新后的名称。在此之前，并不在另一台 Dominion KX II 上更新此名称。

端口状态和可用性

更新 Dominion KX II Port Access（端口访问）页显示的端口状态（Up [工作]或 Down [停止]），说明 CIM 是否通电并连接 Dominion KX II 端口。

更新 Dominion KX II Port Access（端口访问）页显示的端口可用性（Idle [空闲]、Busy [忙]或 Connected [已连接]），只说明在同一台 Dominion KX II 上启动的目标服务器的活动。

如果目标服务器已连接其他 Dominion KX II，只有在尝试建立连接时才检查可用性。拒绝或允许访问，与在 Dominion KX II 上启用的 PC 共享策略保持一致。在此之前，并不在另一台 Dominion KX II 上更新可用性。

如果由于目标服务器忙而拒绝访问，就显示通知。

在 CC-SG 上操作



在 CC-SG 上发出的操作建立在受管 Dominion KX II 报告的状态、可用性和 CIM 名称之上。当目标服务器连接两台受管 Dominion KX II 并给 CC-SG 添加设备时，创建两个节点，每个节点有与之关联的 oob-kvm 接口。也可以在每个 Dominion KX II 上给一个节点配置一个 oob-kvm 接口。

如果给 Dominion KX II 配置 Private（独占）模式，在尝试建立第二个连接时，通知用户不能建立连接并拒绝访问。

在 CC-SG Port Profile（端口配置文件）面板上更改端口名称时，把更改后的名称推送到受管的 Dominion KX II。在尝试通过另一台 Dominion KX II 的 oob-kvm 接口连接目标服务器之前，不在 CC-SG 上更新另一台 Dominion KX II 的相应端口名称。

Dominion KX II 到 Paragon II 配置原则

P2CIM-APS2DUAL 或 P2CIM-AUSBDUAL 可以连接 Dominion KX II 和 Paragon II。

并发访问

必须给 Dominion KX II 和 Paragon II 配置相同的目标服务器并发访问策略。

Paragon II 操作模式	**模式说明**	**支持？**
独占	一个特定通道端口连接的一台服务器或其他设备，每次只能供一个用户采用独占方式访问。	支持。 Paragon II 和 Dominion KX II 必须设置为 Private（独占）模式。Private（独占）设置应用于 Dominion KX II 设备，而不是根据用户组应用。 Paragon II 显示红色表示忙，显示绿色表示可用。
PC 共享	一个特定通道端口连接的一台服务器或其他设备可供多个用户访问，但每次只有一个用户拥有键盘和鼠标控制权。	支持。 但不支持在 Paragon II 上配置的 PC Share Idle Timeout（PC 共享空闲超时）。二者都有并发键盘和鼠标控制权。



Paragon II 操作模式	模式说明	支持？
		Paragon II 显示绿色表示可用。如果另一个用户正在访问目标服务器，也是如此。
公共查看	当一个用户正在访问一个特定通道端口连接的一台服务器或其他设备时，其他用户可以选择此通道端口观看此设备的视频输出。但在他们断开连接或切换到其他目标服务器之前，只有第一个用户拥有键盘和鼠标控制权。	不支持。 在把 CIM 连接到 Paragon II 和 Dominion KX II 时，不能使用此模式。 Paragon II 显示黄色表示它处于 P-View（公共查看）模式。

CIM 名称更新

- 在 Paragon II 上更新的 CIM 名称存储在 Paragon 命名常规对应的 CIM 存储单元里，并在此检索它。
- 在 Dominion KX II 上更新的 CIM 名称存储在 Dominion KX II 命名常规对应的 CIM 存储单元里，并在此检索它。
- 不在 Paragon II 和 Dominion KX II 之间广播 CIM 名称更新。

支持的操作系统（客户机）

Virtual KVM Client 和 Multi-Platform Client (MPC) 支持下列操作系统：

客户机操作系统	客户机支持虚拟媒体
Windows 7®	是
Windows XP®	是
Windows 2008®	是
Windows Vista®	是
Windows 2000 SP4® Server	是
Windows 2003® Server	是



客户机操作系统	客户机支持虚拟媒体
Windows 2008® Server	是
Red Hat® Desktop 5.0	是。在本地保存 ISO 镜像文件，在 Dominion KX II 上直接安装远程文件服务器。
Red Hat Desktop 4.0	是。在本地保存 ISO 镜像文件，在 Dominion KX II 上直接安装远程文件服务器。
Open SUSE 10, 11	是。在本地保存 ISO 镜像文件，在 Dominion KX II 上直接安装远程文件服务器。
Fedora® 8 - 11	是。在本地保存 ISO 镜像文件，在 Dominion KX II 上直接安装远程文件服务器。
Mac® OS	不
Solaris™	不

JRE™ 插件可用于 32 位和 64 位 Windows® 操作系统。只能在 32 位浏览器或 64 位 IE7 或 IE8 浏览器上启动 MPC 和 VKC。

下表列出 Java 32 位和 64 位 Windows 操作系统的 Java™ 要求。

模式	操作系统	**Browser**
Windows x64 32 位模式	Windows XP®	• Internet Explorer® 6.0 SP1+/7.0/IE 8 • Mozilla® 1.4.X 或 1.7+ • Netscape® 7.X • Firefox® 1.06 - 3



模式	操作系统	Browser
	Windows Server 2003®	• Internet Explorer 6.0 SP1++, IE 7, IE 8 • Mozilla 1.4.X 或 1.7+ • Netscape 7.X • Firefox 1.06 - 3
	Windows Vista®	• Internet Explorer 7.0 或 8.0
	Windows 7®	• Internet Explorer 7.0 或 8.0 • Firefox 1.06 - 3
Windows x64 64 位模式	Windows XP	64 位操作系统、 32 位浏览器： • Internet Explorer 6.0 SP1+/7.0/8.0 • Mozilla 1.4.X 或 1.7+ • Netscape 7.X • Firefox 1.06 - 3 64 位模式、 64 位浏览器： • Internet Explorer 7.0 或 8.0
	Windows XP Professional®	
	Windows XP Tablet®	
	Windows Vista	
	Windows Server 2003	
	Windows Server 2008	
	Windows 7	

支持的浏览器

Dominion KX II 支持下列浏览器：

- Internet Explorer® 6/7/8
- Firefox® 1.5/2.0/3.0（最高 build 3.0.10）
- Mozilla® 1.7
- Safari® 2.0



通过认证的调制解调器

- USRobotics® 56K 5686E
- ZOOM® v90
- ZOOM v92
- USRobotics Sportster® 56K
- USRobotics Courier™ 56K

KX2-832 和 KX2-864 扩展本地端口支持的设备

扩展本地端口支持来自下列设备的连接：

- KX2-832 和 KX2-864。
- 直接连接扩展本地端口的 Paragon II 用户工作站 (P2-UST)。
- 直接连接扩展本地端口的 Paragon II 增强型用户工作站 (P2-EUST)。
- 直接连接扩展本地端口的 Cat5Reach URKVMG Receiver。
- 直接连接扩展本地端口的 Paragon II 模拟 KVM 切换器 (UMT) 目标服务器端口。在与 Paragon II 增强型用户工作站一起使用时，提供最大距离的扩展本地端口。

目标服务器连接距离和视频分辨率

最大支持距离是许多因素的函数，包括五类电缆类型/质量、服务器类型和制造商、显卡驱动程序和监视器、环境条件和用户期望值。下表概述各种视频分辨率和刷新率对应的最大目标服务器距离：

视频分辨率	刷新率	最大距离
1600x1200	60	50 英尺 (15m)
1280x1024	60	100 ft (30 m)
1024x768	60	150 英尺 (45m)

注意：由于服务器制造商和服务器类型很多，操作系统版本很多，显卡驱动程序很多，视频质量评判存在主观性，Raritan 不能保证在所有环境下达到所有距离要求。

参看*支持的视频分辨率* (p. 268)，了解 Dominion KX II 支持的视频分辨率。



KX2-832 和 KX2-864 扩展本地端口建议的最大距离

扩展设备	1024x768, 60Hz	1280x1024, 60Hz
使用 EUST 的 Paragon II UMT	1000	900
Paragon EUST	500	400
URKVM	650	250
Paragon UST	500	200

远程连接

远程连接	详细信息
Network（网络）	10BASE-T、100BASE-T 和 1000BASE-T (Gigabit) Ethernet
协议	TCP/IP、UDP、SNTP、HTTP、HTTPS、RADIUS 和 LDAP/LDAPS

支持的视频分辨率

确保 Dominion KX II 支持每台服务器的视频分辨率和刷新率，而且信号是逐行扫描。

视频分辨率和电缆长度是实现鼠标同步的两个重要因素。参看*目标服务器连接距离和视频分辨率* (p. 267)。

Dominion KX II 支持下列分辨率：

分辨率	
640x350 @70Hz	1024x768 @75Hz
640x350 @85Hz	1024x768 @90Hz
640x400 @56Hz	1024x768 @100Hz
640x400 @84Hz	1152x864 @60Hz
640x400 @85Hz	1152x864 @70Hz
640x480 @60Hz	1152x864 @75Hz
640x480 @66.6Hz	1152x864 @85Hz



分辨率	
640x480 @72Hz	1152x870 @75.1Hz
640x480 @75Hz	1152x900 @66Hz
640x480 @85Hz	1152x900 @76Hz
720x400 @70Hz	1280x720@60Hz
720x400 @84Hz	1280x960 @60Hz
720x400 @85Hz	1280x960 @85Hz
800x600 @56Hz	1280x1024 @60Hz
800x600 @60Hz	1280x1024 @75Hz
800x600 @70Hz	1280x1024 @85Hz
800x600 @72Hz	1360x768@60Hz
800x600 @75Hz	1366x768@60Hz
800x600 @85Hz	1368x768@60Hz
800x600 @90Hz	1400x1050@60Hz
800x600 @100Hz	1440x900@60Hz
832x624 @75.1Hz	1600x1200 @60Hz
1024x768 @60Hz	1680x1050@60Hz

注意：复合同步视频和绿色同步视频需要额外的适配器。

注意：可能默认不支持某些分辨率。如果看不到分辨率，先插上监视器电源插头，然后拔掉插头，再插上 CIM。

注意：如果不显示 1440x900 和 1680x1050 分辨率，但目标服务器的显示卡支持这两种分辨率，可能需要使用 DDC-1440 或 DDC-1680 适配器。

支持的键盘语言

Dominion KX II 支持下表列出的键盘语言。

*注意：中文键盘、日文键盘和朝鲜文键盘仅用于显示；Dominion KX II Local Console 功能目前不支持本地语言输入。参看***参考资料** *(p. 285)进一步了解非英文键盘。*

注意：如果使用 Linux 操作系统，Raritan 强烈建议你用系统配置的键盘更改语言。

语言	地区	键盘布局
US English（	美国和大多数英语国家，例如加拿	美国键盘布局



语言	地区	键盘布局
美国英语）	大、澳大利亚和新西兰	
US English International（美国英语国际）	美国和大多数英语国家，例如荷兰	美国键盘布局
UK English（英国英语）	英国	英国键盘布局
繁体中文	香港和台湾	繁体中文
简体中文	中国大陆	简体中文
朝鲜文	韩国	朝鲜文
日文	日本	JIS 键盘
法文	法国	法文 (AZERTY) 键盘布局
德文	德国和奥地利	德文键盘 (QWERTZ) 布局
比利时	比利时	比利时
挪威文	挪威	挪威文
丹麦文	丹麦	丹麦文
瑞典文	瑞典	瑞典文
匈牙利文	匈牙利	匈牙利文
斯洛文尼亚文	斯洛文尼亚	斯洛文尼亚文
意大利文	意大利	意大利文
西班牙文	西班牙和大多数西班牙语国家	西班牙文
葡萄牙文	葡萄牙	葡萄牙文

智能卡读卡器

支持的和不支持的智能卡读卡器

KX II 只支持 USB 型外置智能卡读卡器。

支持的智能卡读卡器



类型	供应商	型号	认证
USB	SCM Microsystems	SCR331	本地和远程认证
USB	ActivIdentity®	ActivIdentity USB Reader v2.0	本地和远程认证
USB	ActivIdentity	ActivIdentity USB Reader v3.0	本地和远程认证
USB	Gemalto®	GemPC USB-SW	本地和远程认证
集成 USB 键盘/读卡器	Dell®	USB Smart Card Reader Keyboard	本地和远程认证
集成 USB 键盘/读卡器	Cherry GmbH	G83-6744 SmartBoard	本地和远程认证
SIM 尺寸智能卡 USB 读卡器	Omnikey	6121	本地和远程认证
集成 (Dell Latitude D620)	O2Micro	OZ776	仅远程
PCMCIA	ActivIdentity	ActivIdentity PCMCIA Reader	仅远程
PCMCIA	SCM Microsystems	SCR243	仅远程

注意：SCM Microsystems SCR331 智能卡读卡器必须使用 SCM Microsystems v5.25 固件。

不支持的智能卡读卡器

下表列出 Raritan 用 KX II 测试过的读卡器，我们发现它们不能正常工作，所以不支持这些读卡器。如果智能卡读卡器不在支持的智能卡读卡器表和不支持的智能卡读卡器表上，Raritan 不能保证它能与 KX II 一起工作。

类型	供应商	型号	备注
集成 USB 键盘/读卡器	HP®	ED707A	无中断终端 => 不兼容 Microsoft® 驱动程序
集成 USB 键盘/读卡器	SCM Microsystems	SCR338	专用读卡器实现技术（不符合 CCID 规范）
USB 令牌	Aladdin®	eToken PRO™	专用实现技术

最低系统要求

本地端口要求

通过本地端口连接 Dominion KX II 的基本互操作要求：

- 在本地连接的所有设备（智能卡读卡器或令牌）必须符合 USB CCID 规范。

目标服务器要求

在使用智能卡读卡器时，目标服务器的基本互操作要求是：

- IFD（智能卡读卡器）控制器必须是标准 USB CCID 设备驱动程序（与通用的 Microsoft USB CCID 驱动程序相当）。
- 需要 D2CIM-DVUSB（双虚拟媒体 CIM），必须使用 3A6E 或更高版本的估计。
- 支持刀片服务器机箱连接，每个刀片使用一个 CIM。
- 只有启用了自动发现功能的 IBM® BladeCenter® H 型和 E 型支持刀片服务器机箱连接，每个机箱使用一个 CIM。

Windows XP 目标服务器

Windows XP® 操作系统目标服务器必须运行 Windows XP SP3，才能同时使用智能卡和 Dominion KX II。如果在目标服务器 Windows XP 环境下使用 .NET 3.5，必须使用 SP1。

Linux 目标服务器

如果使用 Linux® 目标服务器，必须满足下列要求，才能同时使用智能卡读卡器和 Dominion KX II。

- CCID 要求

  如果 Linux 目标服务器不把 Raritan D2CIM-DVUSB VM/CCID 视为智能卡读卡器，可能必须把 CCID 驱动程序升级到 1.3.8 或更高版本，并升级驱动程序配置文件 (Info.plist)。

操作系统	CCID 要求
RHEL 5	ccid-1.3.8-1.el5
SuSE 11	pcsc-ccid-1.3.8-3.12
Fedora® Core 10	ccid-1.3.8-1.fc10.i386



远程客户机要求

远程客户机基本互操作要求是：

- IFD（智能卡读卡器）控制器必须是符合 PC/SC 规范的设备驱动程序。
- 必须能使用 ICC（智能卡）资源管理器，它必须符合 PC/SC 规范。
- JRE™ 1.6.x 和智能卡 API 必须可供 Raritan 客户机应用程序使用。

Linux 客户机

如果使用 Linux® 客户机，必须满足下列要求，才能同时使用智能卡读卡器和 Dominion KX II。

注意：如果有一个或多个目标服务器 KVM 会话处于活动状态，用户插入智能卡登录到客户机所需的时间可能较长。同时正在向这些目标登录。

- PC/SC 要求

操作系统	要求的 PC/SC
RHEL 5	pcsc-lite-1.4.4-0.1.el5
SuSE 11	pcsc-lite-1.4.102-1.24
Fedora® Core 10	pcsc-lite-1.4.102.3.fc10.i386

- 创建 Java™ 库链接

  在升级到 RHEL 4、RHEL 5 和 FC 10 之后，必须创建 libpcsclite.so 软链接，例如 ln –s /usr/lib/libpcsclite.so.1 /usr/lib/libpcsclite.so，假定安装包把库安装在 /usr/lib or /user/local/lib 文件夹里。

- PC/SC 后台进程

  在重新启动 pcsc 后台进程（框架资源管理器）时，同时重新启动浏览器和 MPC。

使用的 TCP 端口和 UDP 端口

端口	说明
HTTP，端口 80	可以按需要配置此端口。参看 ***HTTP 和 HTTPS 端口设置*** (p. 136)。为安全起见，Dominion KX II 把通过 HTTP（端口 80）接收到的所有请求自动转发到 HTTPS。在保证安全的情况下，为方便用户起见，Dominion KX II 响应端口 80，用户不必明确输入 URL 地址即可访问 Dominion KX II。
HTTPS，端口 443	可以按需要配置此端口。参看 ***HTTP 和 HTTPS 端口设置*** (p. 136)。此端口用于实现多个目的，包括 HTML 客户机使用的 Web 服务器，把客户机软件 (MPC/KVC) 下载到客户机的主机上，把 KVM 数据流和虚拟媒体数据流传输到客户机上。
Dominion KX II (Raritan KVM-over-IP) 协议，可配置端口 5000	此端口用于发现其他 Dominion 设备，在 Raritan 设备和系统（包括 CC-SG）之间通信。此端口默认设置为端口 5000，但可以配置它使用当前空闲的任何 TCP 端口。如要详细了解如何配置此设置，参看网络设置。
SNTP（时间服务器），可配置 UDP 端口 123	Dominion KX II 有一个可选功能，使内部时钟与中央时间服务器同步。此功能要求使用 UDP 端口 123（SNTP 标准端口），但也可以配置它使用你指定的任何端口。**可选**
LDAP/LDAPS，可配置端口 389 或 636	如果配置 Dominion KX II 用 LDAP/LDAPS 协议远程验证用户登录，将使用端口 389 或 636，但也可以配置系统使用你指定的任何端口。**可选**
RADIUS，可配置端口 1812	如果配置 Dominion KX II 用 RADIUS 协议远程验证用户登录，将使用端口 1812，但也可以配置系统使用你指定的任何端口。**可选**
RADIUS 记帐，可配置端口 1813	如果配置 Dominion KX II 用 RADIUS 协议远程验证用户登录，同时把 RADIUS 记帐用于事件日志记录，将用端口 1813 或你指定的其他端口传输日志通知。
SYSLOG，可配置 UDP 端口 514	如果配置 Dominion KX II 将消息发送到系统日志服务器，将用指定端口通信，即 UDP 端口 514。
SNMP 默认 UDP 端口	端口 161 用于入站/出站读写 SNMP 访问，端口 162 用于 SNMP 陷阱出站流量。**可选**
TCP 端口 21	端口 21 用于 Dominion KX II 命令行界面（在与 Raritan 技术支持部门一起工作时）。



网络速度设置

Dominion KX II 网络速度设置

网络切换端口设置	自动	**1000/全双工**	**100/全双工**	**100/半双工**	**10/全双工**	**10/半双工**
自动	最高可用速度	1000/全双工	Dominion KX II：100/全双工 切换器：100/半双工	100/半双工	Dominion KX II：10/全双工 切换器：10/半双工	10/半双工
1000/全双工	1000/全双工	1000/全双工	没有通信	没有通信	没有通信	没有通信
100/全双工	Dominion KX II：100/半双工 切换器：100/全双工	Dominion KX II：100/半双工 切换器：100/全双工	100/全双工	Dominion KX II：100/半双工 切换器：100/全双工	没有通信	没有通信
100/半双工	100/半双工	100/半双工	Dominion KX II：100/全双工 切换器：100/半双工	100/半双工	没有通信	没有通信
10/全双工	Dominion KX II：10/半双工 切换器：10/全双工	没有通信	没有通信	没有通信	10/全双工	Dominion KX II：10/半双工 切换器：10/全双工
10/半双工	10/半双工	没有通信	没有通信	没有通信	Dominion KX II：10/全双工 切换器：10/半双工	10/半双工



图注：

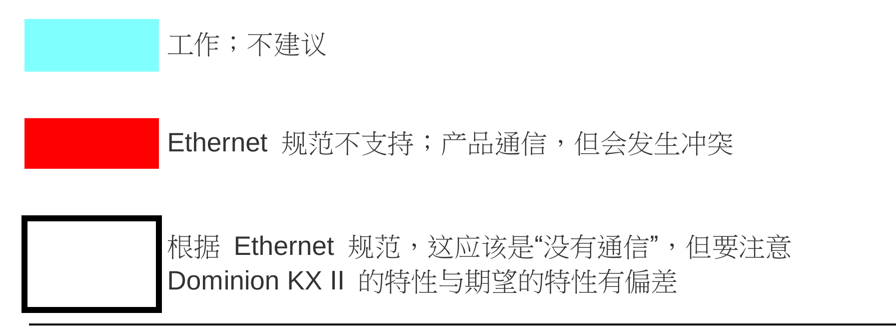
不像期望的那样工作





支持





注意：为了进行可靠网络通信，配置 Dominion KX II 和 LAN 交换机使用相同的 LAN 接口速度和双工。例如将 Dominion KX II 和 LAN 交换机均配置为 Autodetect（自动检测，建议配置），或者设置为 100Mbps/全双工等固定速度/双工。



Ap B 更新 LDAP 模式

注意：只有经验丰富的用户应尝试本章所述的步骤。

在本章内

返回用户组信息

在成功验证之后，用本节中的信息返回用户组信息（有助于授权）。

自 LDAP

当 LDAP 验证成功时，Dominion KX II 根据给定用户组的权限确定他/她的权限。远程 RADIUS 服务器可以返回一个如下所述的属性，从而提供这些用户组名称：

rciusergroup 属性类型：字符串

这可能需要 LDAP/LDAPS 服务器上的模式扩展。请验证服务器管理员启用此属性。

自 Microsoft Active Directory

注意：仅供有经验的 Active Directory® 管理员尝试使用。

在从 Windows® 2000 Server 上的 Microsoft® Active Directory 返回用户组信息时，需要更新 LDAP/LDAPS 模式。参看 Microsoft 文档了解详情。

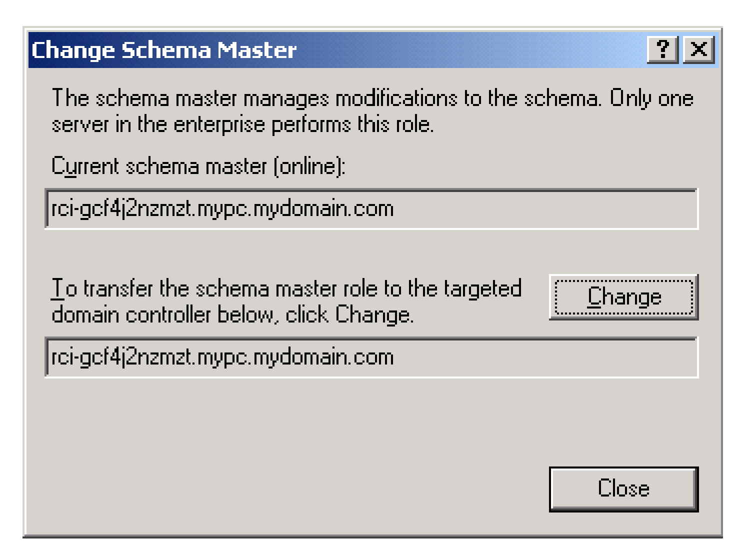
1. 安装 Active Directory 模式插件。参看 Microsoft Active Directory 文档了解说明。
2. 运行 Active Directory Console（Active Directory 控制台），选择 Active Directory Schema（Active Directory 模式）。

设置注册表，允许对模式执行写操作

为了让域控制器写入模式，必须设置一个注册表项允许更新模式。

▶ 允许对模式执行写操作：

1. 用右键单击窗口左面板上的 Active Directory® Schema 根节点，然后单击 Operations Master（主操作）。打开 Change Schema Master（更改主模式）对话框。



2. 选择 Schema can be modified on this Domain Controller（可以在此域控制器上修改模式）复选框。**可选**
3. 单击 OK（确定）按钮。

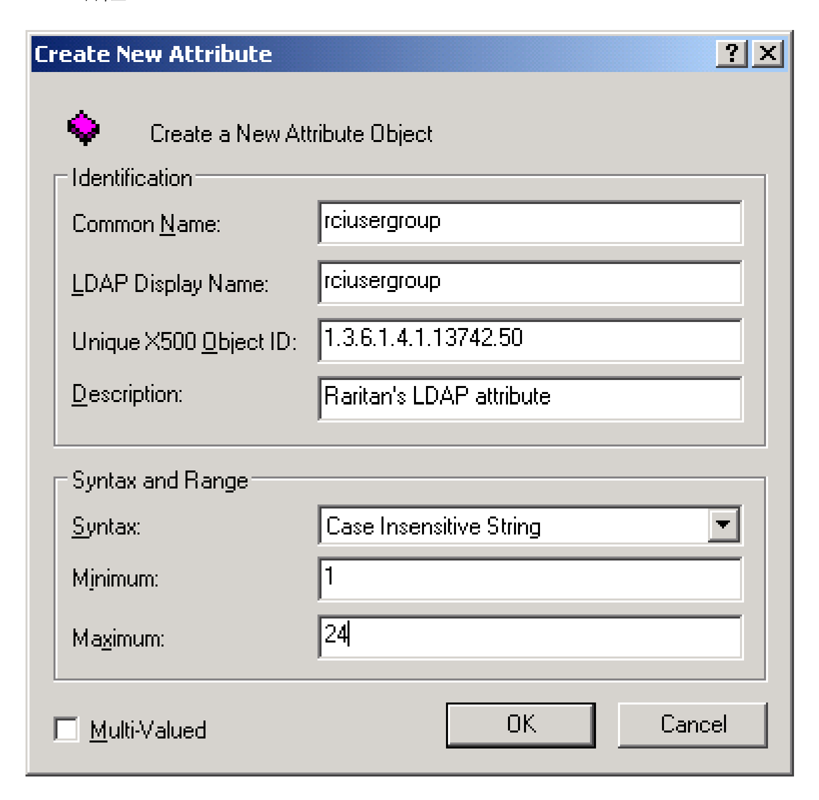
创建新属性

▶ **给 rciusergroup 类创建新属性：**

1. 单击窗口左面板上 Active Directory® Schema 前面的 + 号。
2. 用右键单击左面板上的 Attributes（属性）。



3. 单击 New（新建），然后选择 Attribute（属性）。在显示警告消息时，单击 Continue（继续）按钮，打开 Create New Attribute（创建新属性）对话框。



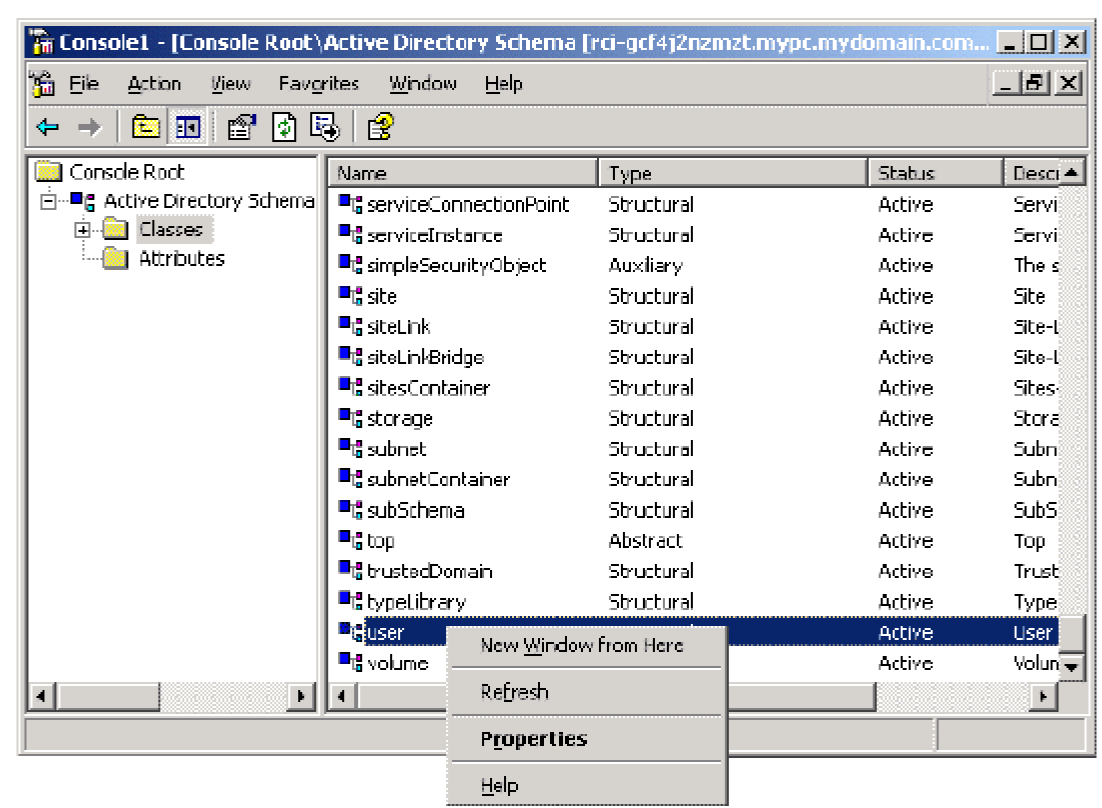
4. 在 Common Name（公用名）字段里输入 *rciusergroup*。
5. 在 LDAP Display Name（LDAP 显示名称）字段里输入 *rciusergroup*。
6. 在 Unique x5000 Object ID（唯一 x5000 对象 ID）字段里输入 *1.3.6.1.4.1.13742.50*。
7. 在 Description（说明）字段里输入有意义的说明。
8. 单击 Syntax（语法）下拉箭头，在列表上选择 Case Insensitive String（不区分大小写的字符串）。
9. 在 Minimum（最小值）字段里输入 *1*。
10. 在 Maximum（最大值）字段里输入 *24*。
11. 单击 OK（确定）按钮创建新属性。

给类添加新属性

▶ 给类添加新属性：

1. 单击窗口左面板上的 Classes（类）。

2. 在右面板上找到用户类，用右键单击它。



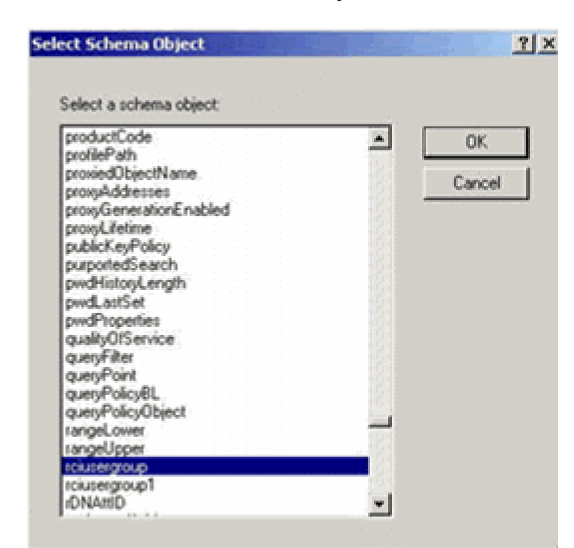
3. 在菜单上选择 Properties（属性）。打开 User Properties（用户属性）对话框。

4. 单击 Attributes（属性）选项卡打开它。

5. 单击 Add（添加）按钮。



6. 在 Select Schema Object（选择模式对象）列表上选择 rciusergroup。



7. 单击 Select Schema Object（选择模式对象）对话框上的 OK（确定）按钮。
8. 单击 User Properties（用户属性）对话框上的 OK（确定）按钮。

更新模式高速缓存

▶ 更新模式高速缓存：

1. 用右键单击窗口左面板上的 Active Directory® Schema，选择 Reload the Schema（重新加载模式）。
2. 最小化 Active Directory Schema MMC (Microsoft® Management Console) 控制台。

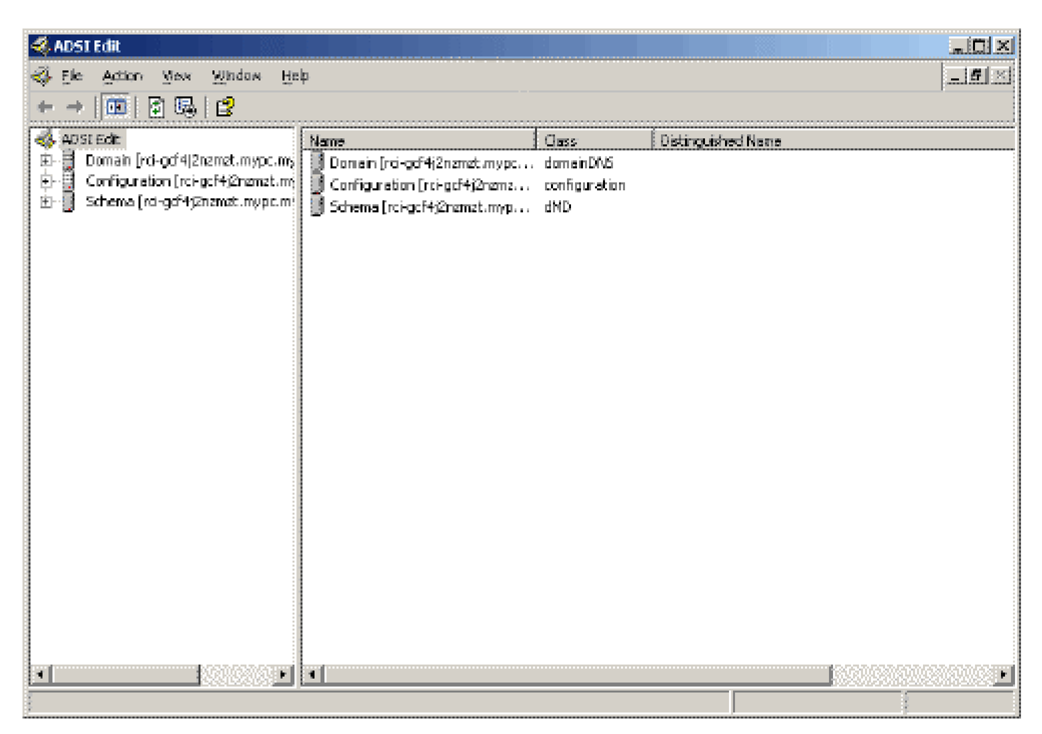
编辑用户成员的 rciusergroup 属性

如要在 Windows 2003® Server 上运行 Active Directory® 脚本，使用 Microsoft® 提供的脚本（在 Windows 2003 Server 安装 CD 上）。在安装 Microsoft Windows 2003 时，将这些脚本加载到系统上。ADSI (Active Directory Service Interface) 充当低级 Active Directory 编辑器，允许你利用目录服务执行添加对象、删除对象和移动对象等常见管理任务。

▶ 编辑组 rciusergroup 的个别用户属性：

1. 在安装 CD 上选择 Support（支持）> Tools（工具）。
2. 双击 SUPTOOLS.MSI 安装支持工具。

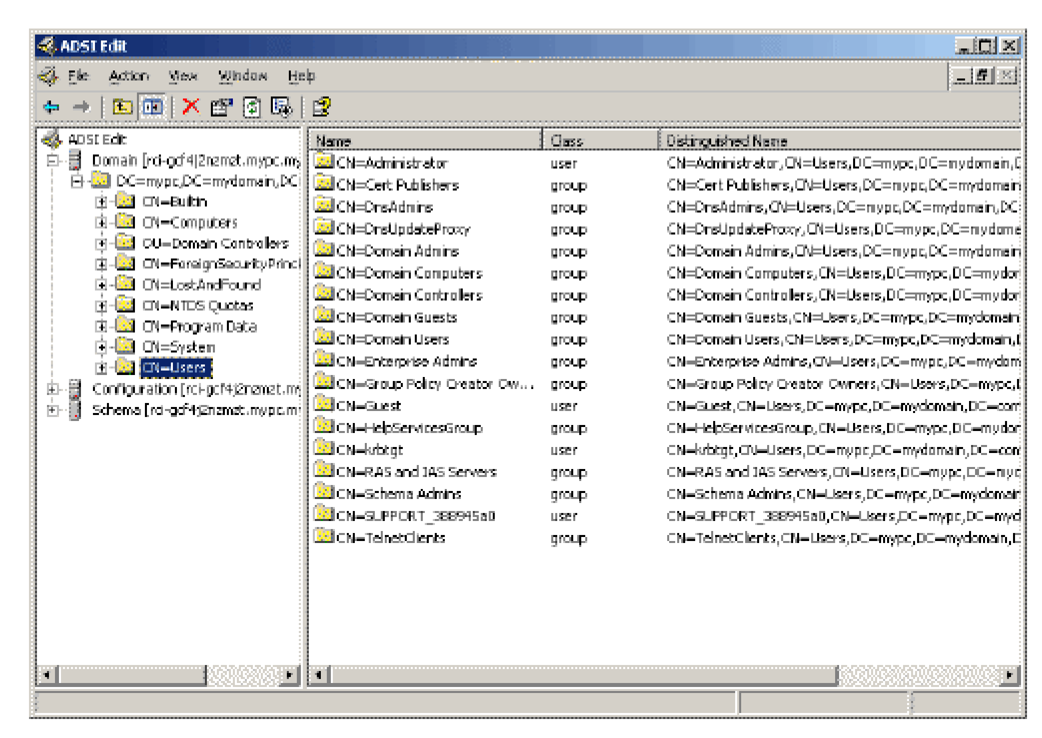
3. 进入支持工具安装目录，运行 adsiedit.msc。打开 ADSI Edit（ADSI 编辑）窗口。



4. 打开 Domain（域）。



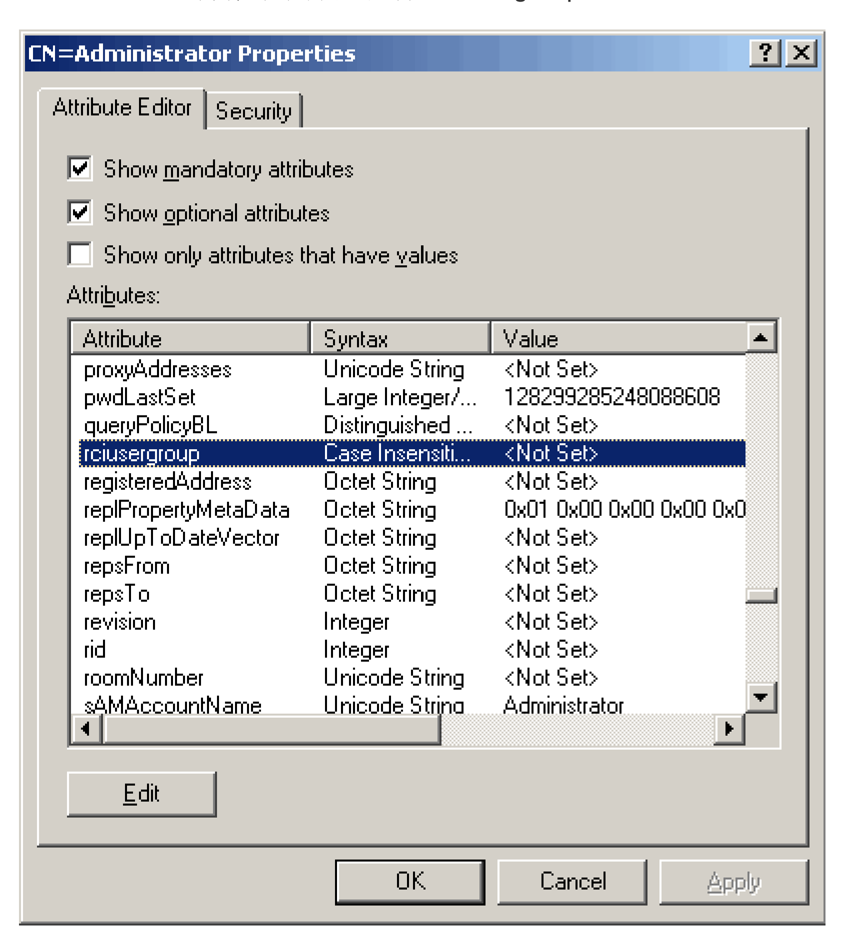
5. 在窗口左面板上选择 CN=Users 文件。



6. 在右面板上找到要调节其属性的用户名。用右键单击用户名，选择 Porperties（属性）。

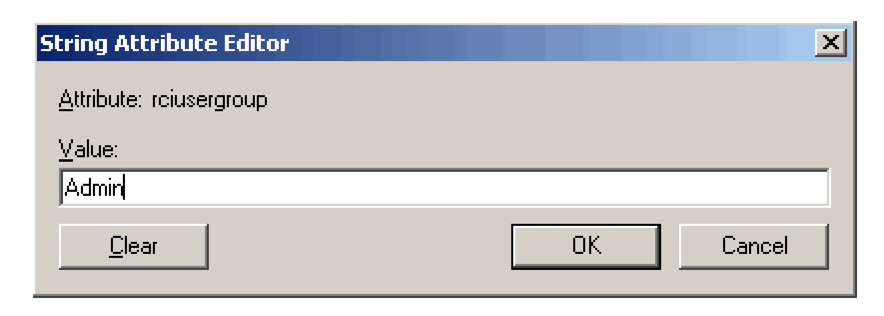


7. 如果 Attribute Editor（属性编辑器）选项卡已经打开了，单击它。在 Attributes（属性）列表上选择 rciusergroup。



8. 单击 Edit（编辑）按钮。打开 String Attribute Editor（字符串属性编辑器）对话框。

9. 在 Edit Attribute（编辑属性）字段里输入（在 Dominion KX II 上创建的）用户组。单击 OK（确定）按钮。





Ap C　参考资料

在本章内

概述

本节重点说明在使用 Dominion KX II 时的注意事项。将记录未来升级，可通过 Dominion KX II Remote Console 界面的 Help（帮助）链接查看升级信息。

Java Runtime Environment (JRE)

重要说明：建议你禁用 Java™ 高速缓存，并清除 Java 高速缓存。请阅读 Java 文档或 KVM 和串行访问客户机指南了解详情。

Dominion KX II Remote Console 和 MPC 需要 Java Runtime Environment™ (JRE) 才能正常工作。Dominion KX II Remote Console 检查 Java 版本。如果版本错误或陈旧，系统会提示你下载兼容版本。

Raritan 建议你用 JRE v1.6 优化性能，但 Dominion KX II Remote Console 和 MPC 可以使用 JRE v1.6.x 和更高版本，1.6.2 除外。

注意：为了在 Dominion KX II Remote Console (Virtual KVM Client) 上使用多语言键盘，要安装多语言版本的 JRE。



IPv6 支持注意事项

Java

Java™ 1.6 在下列平台上支持 IPv6：

- Solaris™ 8 和更高版本
- Linux® kernel 2.1.2 和更高版本（RedHat 6.1 和更高版本）

Java 5.0 和更高版本在下列平台上支持 IPv6：

- Solaris 8 和更高版本
- Linux kernel 2.1.2 和更高版本（为了更好地支持 IPv6，建议使用 kernel 2.4.0 和更高版本）
- Windows XP® SP1、Windows 2003® 和 Windows Vista® 操作系统

Java 不支持下列 IPv6 配置：

- J2SE 1.4 在 Microsoft® Windows® 上不支持 IPv6。

Linux

- 在使用 IPv6 时，建议你使用 Linux kernel 2.4.0 或更高版本。
- 必须安装支持 IPv6 的 kernel，或者必须启用 IPv6 选项重构 kernel。
- 在使用 IPv6 时，还必须安装几个网络工具。参看 http://www.bieringer.de/linux/IPv6/IPv6-HOWTO/IPv6-HOWTO.html 了解详情。

Windows

- Windows XP 和 Windows 2003 用户必须安装 Microsoft IPV6 服务包启用 IPV6。

Mac Leopard

- 对于 Mac® Leopard®，Dominion KX II v2.0.20 不支持 IPv6。

Samba

- 在使用 Samba 时，虚拟媒体不支持 IPv6。



键盘

非英文键盘

法文键盘

^ 符号（仅 Linux® 客户机）

当 Linux 客户机使用法文键盘时，Virtual KVM Client 和 Multi-Platform Client (MPC) 不将 Alt Gr+9 组合键当作 ^ 符号处理。

▶ 输入 ^ 符号：

按法文键盘上的 ^ 键（位于 P 键右边），立刻按 spacebar。

也可以创建一个由下列命令构成的宏：

1. 按住右 Alt
2. 按 9
3. 释放 9
4. 释放右 Alt

注意：这些步骤不适用于（元音上的）抑扬音符号。在所有情况下，可以用法文键盘上的 ^ 键（位于 P 键右边）与另一个字符组合起来，输入抑扬音符号。

重音符号（仅 Windows XP® 操作系统客户机）

当 Windows XP 客户机使用法文键盘时，在 Virtual KVM Client 和 Multi-Platform Client 上输入 Alt Gr+7 组合键，即可输入重音符号，但显示两个符号。

注意：Linux 客户机不会发生这种情况。

数字键盘

在使用法文键盘时，在 Virtual KVM Client 和 Multi-Platform Client 上输入数字键盘符号显示如下：

数字键盘符号	显示为
/	;
.	;



代字号

在使用法文键盘时，在 Virtual KVM Client 和 Multi-Platform Client 上输入 Alt Gr+2 组合键不转换成代字号 (~)。

► 输入代字号：

创建一个由下列命令构成的宏：

- 按住右 Alt
- 按 2
- 释放 2
- 释放右 Alt

键盘语言首选项（Fedora Linux 客户机）

由于在给用 System Preferences（系统首选项）配置的外文键盘生成正确的键事件时， Linux® 运行的 Sun™ JRE™ 有问题，Raritan 建议你用下表所述的方法配置外文键盘。

语言	配置方法
US Intl（美国英语/国际）	默认值
UK（英国英语）	System Settings（系统设置）(Control Center[控制中心])
French（法文）	Keyboard Indicator（键盘指示器）
German（德文）	Keyboard Indicator（键盘指示器）
Hungarian（匈牙利文）	System Settings（系统设置）(Control Center[控制中心])
Spanish（西班牙文）	System Settings（系统设置）(Control Center[控制中心])
Swiss-German（瑞士德文）	System Settings（系统设置）(Control Center[控制中心])
Norwegian（挪威文）	Keyboard Indicator（键盘指示器）
Swedish（瑞典文）	Keyboard Indicator（键盘指示器）
Danish（丹麦文）	Keyboard Indicator（键盘指示器）
Japanese（日文）	System Settings（系统设置）(Control Center[控制中心])
Korean（朝鲜文）	System Settings（系统设置）(Control



语言	配置方法
US Intl（美国英语/国际）	默认值
	Center[控制中心])
Slovenian（斯洛文尼亚文）	System Settings（系统设置）(Control Center[控制中心])
Italian（意大利文）	System Settings（系统设置）(Control Center[控制中心])
Portuguese（葡萄牙文）	System Settings（系统设置）(Control Center[控制中心])

注意：在使用 Gnome 作为桌面环境的 Linux 系统上，应该使用 Keyboard Indicator（键盘指示器）。

在 Linux 客户机上使用匈牙利文键盘时，只有 JRE 1.6 支持带双锐音符号的拉丁字母 Ü 和带双锐音符号的拉丁字母 Ö。

在 Fedora® Linux 客户机上可以采用几种方法设置键盘语言首选项。为了让键正确映射到 Virtual KVM Client 和 Multi-Platform Client (MPC)，必须使用下列方法。

用系统设置功能设置键盘语言：

1. 在工具栏上选择 System（系统）> Preferences（首选项）> Keyboard（键盘）。
2. 打开 Layouts（布局）选项卡。
3. 添加或选择相应的语言。
4. 单击 Close（关闭）按钮。

用键盘指示器设置键盘语言：

1. 用右键单击任务栏，选择 Add to Panel（添加到面板）。
2. 在 Add to Panel（添加到面板）对话框上用右键单击 Keyboard Indicator（键盘指示器），在菜单上选择 Open Keyboard Preferences（打开键盘首选项）。
3. 在 Keyboard Preferences（键盘首选项）对话框上单击 Layouts（布局）选项卡。
4. 按需要添加和删除语言。



Macintosh 键盘

在将 Macintosh® 用作客户机时，Java™ Runtime Environment (JRE™) 不捕捉 Mac® 键盘上的下列键：

- F9
- F10
- F11
- F14
- F15
- Volume Up
- Volume Down
- Mute
- Eject

因此，Virtual KVM Client 和 Multi-Platform Client (MPC) 不能处理在 Mac 客户机键盘上输入的这些键。

鼠标指针同步 (Fedora)

在采用双鼠标模式连接运行 Fedora® 7 的目标服务器时，目标服务器鼠标指针和本地鼠标指针可能过一会儿就不同步了。

▶ 重新同步鼠标光标：

- 使用 Virtual KVM Client 上的 Synchronize Mouse（同步鼠标）选项。

下表概述 Dominion KX II 鼠标模式，以及在访问运行 Fedora 的 KVM 目标服务器时，这些模式是否保持同步：

鼠标模式	Fedora Core 5	Fedora Core 6
绝对鼠标同步	不	不
智能鼠标模式	不	是
标准鼠标模式	是	不



Dell 机箱电缆长度和视频分辨率

为了保持视频质量，Raritan 建议你在 Dominion KX II 上连接 Dell® 刀片服务器机箱时，使用下列电缆长度和视频分辨率：

电缆长度	视频分辨率
50 英尺	1024x768x60
50 英尺	1280x1024x60
30 英尺	1600x1200x60

Fedora

解决 Fedora Core 焦点问题

在使用 Multi-Platform Client (MPC) 时，偶尔不能登录 Dominion KX II 设备，或者不能访问 KVM 目标服务器（Windows®、SUSE 等）。此外，Ctrl+Alt+M 组合键可能不弹出 Keyboard Shortcut（键盘快捷键）菜单。这种情况是下列客户机配置造成的：Fedora® Core 6 和 Firefox® 1.5 或 2.0。

测试表明，安装 libXp 可以解决 Fedora Core 6 存在的窗口聚焦问题。Raritan 用 libXp-1.0.0.8.i386.rpm 进行了测试，可以用它解决所有键盘焦点和弹出菜单问题。

注意：SeaMonkey（以前叫 Mozilla®）浏览器也需要 libXp，才能使用 Java™ 插件。

在 VKC 和 MPC 上用智能卡连接 Fedora 服务器

如果在 MPC 或 VKC 上用智能卡连接 Fedora® 服务器，并在连接之后取出智能卡，在 FC7 和 FC8 服务器上并不释放 pcsc-lite 库，必须重新启动 pcscd 后台进程才能释放它。为了避免出现这种情况，把 pcsc-lite 库升级到 1.4.102-3 或更高版本。

解决在使用 Fedora 服务器时出现的 Firefox 冻结问题

如果访问 Firefox® 并使用 Fedora® 服务器，在打开 Firefox 时可能会出现冻结现象。在服务器上安装 libnpjp2.so Java™ 插件可以解决这个问题。

视频模式和分辨率

SUSE/VESA 视频模式

SuSE X.org 配置工具 SaX2 采用 X.org 配置文件里的模式行项生成视频模式。这些视频模式不精确对应 VESA 视频模式定时（即使选择了 VESA 监视器）。另一方面，Dominion KX II 依靠精确的 VESA 模式定时进行正确同步。这一视差可能会导致黑边，失去图像的几个部分，引入噪声。

配置 SUSE 视频显示：

1. 生成的配置文件 /etc/X11/xorg.conf 包括 Monitor 节，本节有一个名为 UseModes 的选项，例如
   UseModes "Modes[0]"
2. 要么（用 #）备注此行，要么将它删除掉。
3. 重新启动 X 服务器。

在进行此项更改之后，将使用来自 X 服务器的内部视频模式定时，它精确对应 VESA 视频模式定时，使 Dominion KX II 能正常显示视频。

支持的分辨率无法显示

在使用 CIM 时，可能默认无法选择*支持的视频分辨率* (p. 268)列出的部分分辨率。

查看不显示的所有可用视频分辨率：

1. 插上监视器电源插头。
2. 拔掉监视器电源插头，插上 CIM。并非所有视频分辨率都可以选择和使用。

USB 端口和配置文件

VM-CIM 和 DL360 USB 端口

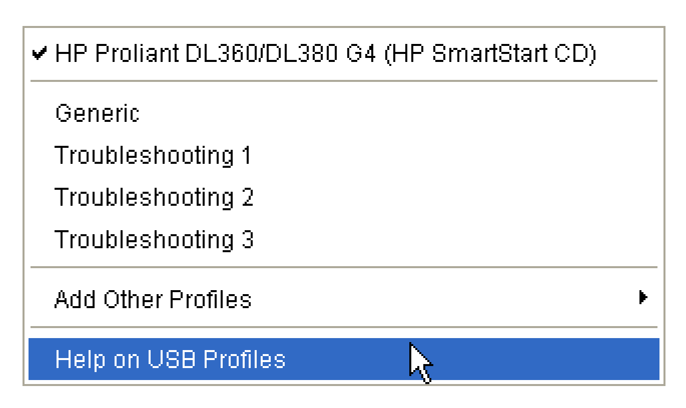
HP® DL360 服务器背板上有一个 USB 端口，面板上还有一个 USB 端口。不能同时使用 DL360 的两个 USB 端口。因此，不能在 DL360 服务器上使用双 VM-CIM。

但是，如果将 USB2 集线器作为工作区连接到设备背板上的 USB 端口，可以将双 VM-CIM 插入集线器。



USB 配置文件选择帮助

在 VKC 上连接 KVM 目标服务器时，可以通过 USB Profile（USB 配置文件）菜单上的 Help on USB Profiles（USB 配置文件帮助）命令查看 USB 配置文件信息。



USB Profile Help（USB 配置文件帮助）窗口显示 USB 配置文件帮助。如要详细了解特定 USB 配置文件，参看***可用的 USB 配置文件*** (p. 99)。

Raritan 针对众多操作系统级和 BIOS 级服务器实现推出一组标准的 USB 配置文件。这些配置文件旨在使远程 USB 设备配置和目标服务器配置实现最佳匹配。

Generic 配置文件可以满足大多数常部署的目标服务器配置的要求。

还提供其他配置文件满足其他常部署的服务器配置（例如 Linux® 和 Mac OS-X®）的特定要求。

还有许多定制配置文件（用平台名称和 BIOS 版本号命名）可增强目标服务器的虚拟媒体功能，例如在 BIOS 级操作时。

Add Other Profiles（添加其他配置文件）便于你访问系统上可用的其他配置文件。在此列表上选择的配置文件被添加到 USB Profile（USB 配置文件）菜单上。其中包括一组故障排除配置文件，旨在协助你确定配置局限性。

USB Profile（USB 配置文件）菜单选项可以在 Console Device Settings（控制台设备设置）> Port Configuration（端口配置）页上配置。

如果 Raritan 提供的所有标准 USB 配置文件都不满足目标服务器要求，Raritan 技术支持部门可与你一起针对该目标服务器设计定制解决方案。Raritan 建议你：

1. 在 Raritan 网站 (www.raritan.com) 的 Firmware Upgrade（固件升级）页上查看最新版本说明，看看是否有可供你的配置使用的解决方案。
2. 如果没有，请在联系 Raritan 技术支持部门时提供下列信息：
    a. 目标服务器信息、制造商和型号，以及 BIOS、开发商和版本。

b. 指定用途（例如重定向镜像文件，以便重新加载 CD 上的服务器操作系统）。

在使用智能卡读卡器时更改 USB 配置文件

在某些情况下，必须针对目标服务器更改 USB 配置文件。例如在目标服务器发生“高速 USB”连接速度问题时，可能必须把连接速度更改为 Use Full Speed for Virtual Media CIM（针对虚拟媒体 CIM 使用全速）。

在更改配置文件时，可能显示“检测到新硬件”消息，必须凭借管理权限登录到目标服务器才能重新安装 USB 驱动程序。只有在目标服务器最初几次发现 USB 设备的新设置时，才会出现这种情况。在此之后，目标服务器会正确选择驱动程序。

CIM

在 Linux 目标服务器上使用 Windows 三键鼠标

在与 Linux® 目标服务器相连的 Windows® 客户机上使用三键鼠标时，左鼠标按钮可能被映射到 Windows 客户机三键鼠标的中间按钮。

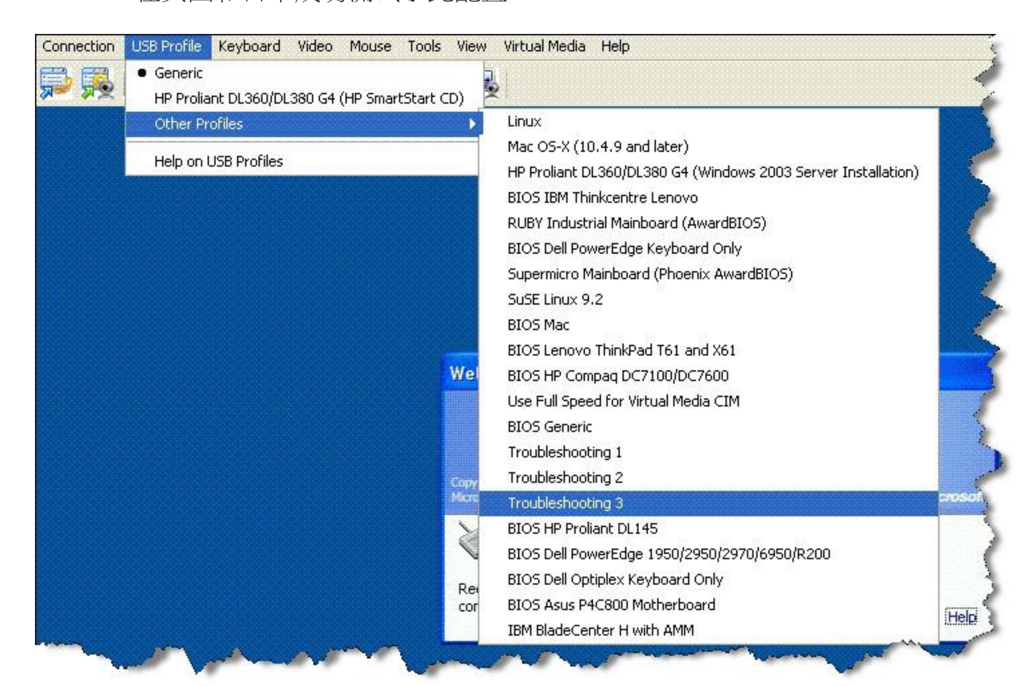


Windows 2000 虚拟媒体 USB 组合设备特性

与 USB 非组合设备一样，Windows 2000® 操作系统不支持 Raritan D2CIM-VUSB 等 USB 组合设备。

因此，对于被 D2CIM-VUSB 映射的驱动器，系统托盘不显示 Safely Remove Hardware（安全拆除硬件）图标，在断开设备时可能显示一条警告消息。Raritan 尚未从此消息上发现任何问题。

Raritan 的美国工程部开发了一个支持 Safely Remove Hardware（安全拆除硬件）图标的配置，不再显示此 Windows 消息。此配置要求使用 D2CIM-DVUSB 虚拟媒体适配器和 Troubleshooting 3 USB Profile，后者将 D2CIM-DVUSB 配置为支持一个虚拟媒体连接的 USB 非组合设备。Raritan 在美国和日本成功测试了此配置。



虚拟媒体

在添加文件之后不刷新虚拟媒体

在安装虚拟媒体驱动器之后，如果给该驱动器添加了文件，目标服务器可能不立刻显示这些文件。断开虚拟媒体连接，然后重新连接虚拟媒体。

用 D2CIM-VUSB 访问 Windows 2000 Server 上的虚拟媒体

不能用 D2CIM-VUSB 访问 Windows 2000® Server 上的虚拟媒体本地驱动器。

使用虚拟媒体时的目标服务器 BIOS 启动时间

如果采用虚拟方式将介质安装在目标服务器上，某些目标服务器的 BIOS 启动时间可能较长。

▶ 缩短启动时间：

1. 关闭 Virtual KVM Client，彻底释放虚拟媒体驱动器。
2. 重新启动目标服务器。

用高速连接虚拟媒体时虚拟媒体连接失败

在某些情况下，如果目标服务器发生“高速 USB”连接问题，或者目标服务器由于增加连接器和电缆（例如通过 dongle 连接刀片服务器）造成的信号衰减而发生 USB 协议错误，可能必须选择 Use Full Speed for Virtual Media CIM（针对虚拟媒体 CIM 使用全速）。

CC-SG

在 CC-SG 代理模式下不知道 Virtual KVM Client 版本

在代理模式下，在 CommandCenter Secure Gateway (CC-SG) 上启动 Virtual KVM Client 时，不知道 Virtual KVM Client 版本。在 About Raritan Virtual KVM Client（关于 Raritan Virtual KVM Client）对话框上，版本显示为 Version Unknown（未知版本）。

单鼠标模式 — 在 VKC 上用 Firefox 连接受 CC-SG 控制的 Dominion KX II 目标服务器

在采用 DCIM-PS2 或 DCIM-USBG2，用 Firefox® 连接受 CC-SG 控制的 Dominion KX II 目标服务器时，如果在 Virtual KVM Client 上更改为 Single Mouse Mode（单鼠标模式），VKC 窗口不再是聚焦窗口，鼠标不响应。如果发生这种情况，单击鼠标左键，后者按 Alt+Tab，即可让 VKC 窗口重新聚焦。

代理模式和 MPC

如果在 CC-SG 配置下使用 Dominion KX II，假如要使用 Multi-Platform Client (MPC)，切勿使用 CC-SG 代理模式。



在 Dominion KX II 的不同端口之间移动

如果在同一台 Dominion KX II 的不同端口之间移动，并在一分钟内恢复管理，CC-SG 可能不显示错误消息。如果恢复管理，将更新显示器显示的信息。

Ap D 常见问题解答

在本章内



一般性问题

Dominion KX II 是什么设备？

Dominion KX II 是第二代 KVM(键盘、视频和鼠标)切换器，允许 1/2/4/8 个 IT 管理员利用 BIOS 级功能通过网络访问和控制 8/16/32/64 台服务器。Dominion KX II 是硬件，与操作系统无关。即使服务器停机了，用户也可以排除服务器故障，并重新配置服务器。

机架安装的 Dominion KX II 具有与传统 KVM 切换器相同的功能，同样很便利，同样节省空间和成本。但 Dominion KX II 还集成了业界性能最好的 KVM-over-IP 技术，使多个管理员可以在任何联网工作站上访问服务器 KVM 控制台。

Dominion KX II 与远程控制软件有何区别？

在远程使用 Dominion KX II 时，界面乍一看很类似远程控制软件，例如 pcAnywhere、Windows Terminal Services/Remote Desktop、VNC 等。但由于 Dominion KX II 不是软件解决方案，而是硬件解决方案，所以它的功能更强。尤其是：

- 独立于操作系统和硬件 – 可以用 Dominion KX II 管理很多运行流行操作系统的服务器，包括运行 Windows®、Linux® 和 Solaris™ 等操作系统的 Intel®、Sun™ 和 PowerPC。
- 独立于状态/无代理 — Dominion KX II 不要求受管服务器的操作系统运行，也不要求在受管服务器上安装任何专用软件。
- 带外 — 即使受管服务器自己的网络连接不可用，仍然可以通过 Dominion KX II 管理它。
- BIOS 级访问 — 即使服务器开机挂起，要求启动进入安全模式，或者要求修改系统 BIOS 参数，Dominion KX II 仍然无故障工作，从而顺利完成这些配置。

Dominion KX II 与 KX I 相比有哪些新功能？

Dominion KX II 有很多令人激动的新功能，包括虚拟媒体、绝对鼠标同步™、双电源、双 Gigabit Ethernet、通用 Web 用户界面、下一代本地端口等。

如何从 Dominion KX I 过渡到 Dominion KX II？

客户通常可以继续使用现有切换器许多年。客户可以随着数据中心膨胀，购买和使用新的 Dominion KX II 产品。Raritan 的集中管理设备 CommandCenter Secure Gateway 和 Multi-Platform Client (MPC) 无缝支持 KX I 和 Dominion KX II 切换器。

现有的 KX I CIM 是否支持 Dominion KX II 切换器？



是，现有的 KX I CIM 支持 Dominion KX II 切换器。此外，精选的 Paragon CIM 也支持 Dominion KX II。这样，如果客户想使用 KVM-over-IP 技术，很容易从 Paragon I 过渡到 Dominion KX II。但你可能想考虑 D2CIM-VUSB 和 D2CIM-DVUSB CIM，它们支持虚拟媒体和绝对鼠标同步。

Dominion KX II 是否可以安装在机架上？

是。Dominion KX II 配备标准的 19" 机架安装托架。它还可以反向安装在机架上，让服务器端口向外。

Dominion KX II 有多大尺寸？

Dominion KX II 只有 1U 高（KX2-864 和 KX2-464 除外，为 2U），适合安装在 19" 标准机架上，深度只有 11.4" (29cm)。Dominion KX2-832 和 KX2-864 的深度为 13.8" (44cm)。



远程访问

多少用户可以同时远程访问每台 Dominion KX II 连接的服务器？

Dominion KX II 设备每个用户通道最多支持八个用户建立远程连接，他们可以同时访问和控制一台目标服务器。对于 DKX2-116 等单通道设备，最多可以让八个远程用户访问和控制一台目标服务器。对于 DKX2-216 等双通道设备，第一个通道最多可以让八个远程用户访问和控制服务器，第二个通道最多可以让另外八个远程用户访问和控制服务器。对于四通道设备，每个通道最多支持八个用户，总共支持 32 (8 x 4) 个用户访问和控制四台服务器。同理，对于八通道设备，最多八个用户可以访问一台服务器，8 个通道最多支持 32 个用户。

两个人是否可以同时看到同一台服务器？

是，实际上最多可以让八个人同时访问和控制任何一台服务器。

两个人是否可以同时访问同一台服务器，其中一个人远程访问服务器，另一个人通过本地端口访问服务器？

是，本地端口完全独立于远程端口。本地端口可以用 PC 共享功能访问同一台服务器。

为了在客户机上访问 Dominion KX II，需要进行哪些硬件配置、软件配置或网络配置？

由于 Dominion KX II 完全可以通过 Web 访问，所以不需要在用于访问的客户机上安装专用软件。可以在 Raritan.com 上下载可选安装的客户机，通过外置调制解调器访问需要它。

Dominion KX II 可以通过主要网络浏览器访问，包括 Internet Explorer、Mozilla 和 Firefox。现在可以通过 Raritan 新推出的 Windows Client、基于 Java 的 Multi-Platform Client 和 Virtual KVM Client，在 Windows、Linux 和 Macintosh 桌面上访问 Dominion KX II。

Dominion KX II 管理员还可以利用便捷的浏览器界面执行远程管理任务（设置密码和安全，重新命名服务器，更改 IP 地址等）。

访问 Dominion KX II 所用的 Virtual KVM Client 小程序文件有多大？下载时间有多长？

访问 Dominion KX II 所用的 Virtual KVM Client 小程序大约有 500kB。下表说明在不同的网络速度下，下载 Dominion KX II 小程序所需的大致时间：

速度	说明	时间
100Mbps	理论上 100MB 网络速度	0.05 秒



速度	说明	时间
60Mbps	实际上可能 100MB 网络速度	0.08 秒
10Mbps	理论上 10MB 网络速度	0.4 秒
6Mbps	实际上可能 10MB 网络速度	0.8 秒
512Kbps	电缆调制解调器下载速度（典型）	8 秒

如果网络不可用，如何访问与 Dominion KX II 相连的服务器？

可以在机架上访问服务器，也通过调制解调器访问服务器。Dominion KX II 有专用调制解调器端口，用于连接外部调制解调器。

Do you have a Windows® client?

有，R2.2 增加了本机 .NET Windows Client，叫做 Raritan Active KVM Client。

是否有非 Windows 客户机？

是。Virtual KVM Client 和 Multi-Platform Client (MPC) 都允许非 Windows 用户通过 Dominion KX I 和 Dominion KX II 切换器连接 KVM 目标服务器。MPC 既可以通过网络浏览器运行，也可以独立运行。参看 **KVM 和串行客户机指南**中的 **Virtual KVM Client** 和 **Raritan Multi-Platform Client (MPC) 支持的操作系统**了解详情。

KVM 客户机是否支持 LCD 监视器？

是。对于那些要在桌面上使用多台 LCD 监视器提高生产力的客户，Dominion KX II 可以按全屏模式或标准模式启动多个与多台监视器的 KVM 会话。

在 Virtual KVM Client 会话过程中，有时 Alt 键似乎不起作用。我该怎么办？

在按住 Alt 键不放时，通常会发生这种情况。例如在按 spacebar 时继续按 Alt 键，屏幕显示可能会从目标服务器切换到客户机 PC。本地操作系统解释此组合键，在活动窗口（客户机 PC）上触发此组合键对应的操作。



通用虚拟媒体

哪些 Dominion KX II 型号支持虚拟媒体？

所有 Dominion KX II 型号都支持虚拟媒体。它们既可以单独支持虚拟媒体，也可以通过 Raritan CommandCenter Secure Gateway 集中管理设备支持虚拟媒体。

Dominion KX II 设备支持哪几种虚拟媒体。

Dominion KX II 支持下列几种虚拟媒体：内置和 USB 连接的 CD/DVD 驱动器、USB 海量存储设备、PC 硬盘和 ISO 镜像文件。

虚拟媒体有什么要求？

需要一个 Dominion KX II 虚拟媒体 CIM。有两种 CIM：D2CIM-VUSB 和新的 D2CIM-DVUSB。

D2CIM-DVUSB 有两个 USB 连接器，供那些要在 BIOS 级使用虚拟媒体的客户使用。进行智能卡验证还需要 D2CIM-DVUSB。

D2CIM-VUSB 有一个单 USB 连接器，供那些要在操作系统级使用虚拟媒体的客户使用。

两种 CIM 都支持与（支持 USB 2.0 接口的）目标服务器进行虚拟媒体会话。

CIM 包装数量有 32 个和 64 个两种，支持绝对鼠标同步和远程固件更新。

虚拟媒体是否安全？

是。虚拟媒体会话用 AES 或 RC4 加密算法加以保护。

USB 配置文件

什么是 USB 配置文件？

为了使用虚拟媒体等 USB 服务，某些服务器需要使用专门配置的 USB 接口。USB 配置文件给服务器定制 Dominion KX II 的 USB 接口，以便适应这些服务器特有的特点。

为什么要使用 USB 配置文件？

最常见的情况是在访问虚拟媒体设备时，如果 BIOS 不全面支持 USB 规范，就要在 BIOS 级使用 USB 配置文件。

但是，有时在操作系统过级使用配置文件是为了实现其他目的，例如使 Mac® 服务器和 Linux® 服务器实现鼠标同步。

如何使用 USB 配置文件？

管理员可以在 Dominion KX II Port Configuration（端口配置）页上配置各个端口或端口组使用特定的 USB 配置文件。

必要时也可以在 Dominion KX II 客户机上选择 USB 配置文件。

如果选择的 USB 配置文件不合适，会发生什么情况？

如果不给 KVM 目标服务器选择合适的 USB 配置文件，不能优化海量存储设备、鼠标或键盘的性能，它们甚至根本不能正常工作。

在使用虚拟媒体时，是否始终要设置 USB 配置文件？

不，在许多情况下，在操作系统级使用虚拟媒体或在 BIOS 级工作但不访问虚拟媒体时，使用默认 USB 配置文件就可以了。

可以使用哪些配置文件？

参看***可用的 USB 配置文件*** (p. 99)。

如何知道哪个 USB 配置文件最适合给定的目标服务器？

Generic 配置文件适合绝大多数目标服务器。如果此配置文件不支持给定的 KVM 目标服务器，可以在***可用的 USB 配置文件*** (p. 99)里选择合适的 USB 配置文件。选择最适合目标服务器的配置文件。

BIOS 配置文件有什么用途？

BIOS 配置文件是定制配置文件，可以满足那些无需实现全 USB 规范的特殊服务器的 BIOS 的要求。这些配置文件克服了 BIOS 存在的限制和局限性，允许你在 BIOS 级使用键盘、鼠标和虚拟媒体。

使用 USB 配置文件是否需要特殊 CIM？



必须使用安装了最新固件的 D2CIM-VUSB 或 D2CIM-DVUSB。

Raritan 是否提供用于其他目标服务器配置的 USB 配置文件？

Raritan 将针对客户需求提供新的 USB 配置文件。在增加新配置文件时，将它们包括在固件升级中。

带宽和 KVM-over-IP 性能

KVM-over-IP 系统如何使用带宽？

Dominion KX II 集成了下一代 KVM-over-IP 技术，即目前最好的视频压缩技术。Raritan 采用的高质量视频传输和低带宽用量技术获得了多项技术大奖。

Dominion KX II 将来自目标服务器的键盘信号、视频信号和鼠标信号进行数字化处理、压缩和加密，通过 IP 网络将 IP 数据包发送到远程客户机，与用户建立远程会话。Dominion KX II 采用业界领先的视频处理算法，使远程访问犹如在机架上访问一样。

屏幕变化（例如视频）占用绝大部分带宽，键盘活动和鼠标活动所用的带宽要小得多。

必须注意只有在用户处于活动状态时，才使用带宽。使用的带宽大小取决于服务器显示屏的变化情况。

如果视频没有变化，即用户不与服务器交互操作，通常不使用带宽。如果用户移动鼠标或输入字符，使用的带宽很小。如果显示器运行复杂的屏幕保护或播放视频，要使用较大的带宽。

带宽对 KVM-over-IP 性能有什么影响？

通常要在带宽和性能之间找到一个平衡点。可用带宽越大，可以实现更好的性能。在带宽很有限的情况下，性能可能会下降。Dominion KX II 经过优化，在众多环境下可以实现很高的性能。

哪些因素影响带宽？

有许多因素决定了要使用多大带宽。如上所述，主要因素是目标服务器显示屏的变化情况。这取决于用户的任务和操作。

其他因素包括服务器视频分辨率、联网速度和特性、客户机 PC 资源和显示卡噪声。

Dominion KX II 用很复杂的视频处理算法优化在多种环境下的带宽和性能。此外，由于可以采用许多设置优化带宽用量，可以全面配置这些因素。尤其是可以在远程客户机（VKC 和 MPC）上设置连接速度，从而降低带宽用量。

与 KX I 不同的是，噪声过滤器参数通常对降低带宽或提高性能没有太大作用。

KX II 执行常见任务需要多大带宽？

带宽取决于用户的任务和操作。服务器显示屏变化越大，使用的带宽越大。



下表概述在 Windows XP 目标服务器（1024x768 分辨率）上，在 100 Mbps LAN 里使用 Dominion KX II 的默认设置和两个降低带宽设置(连接速度设置为 1MB，彩色为 15 位和 8 位）时，某些标准用例：

用户任务	默认值	**1MB 速度 & 15 位彩色**	**1MB 速度 & 8 位彩色**
Idle Windows Desktop	0 Kbps	0 Kbps	0 Kbps
移动鼠标光标	5-15 Kbps	2-16 Kbps	2-3 Kbps
拖动图标	40-70 Kbps	10-25 Kbps	5-15 Kbps
拖动文件夹	10-40 Kbps	5-20 Kbps	5-10 Kbps
打开文本窗口	50-100 Kbps	25-50 Kbps	10-15 Kbps
连续输入字符	1 Kbps	0.5-1 Kbps	0.2-0.5 Kbps
滚动文本窗口	10-50 Kbps	5-25 Kbps	2-10 Kbps
关闭文本窗口	50-100 Kbps	20-40 Kbps	10-15 Kbps
打开面板	50-100 Kbps	60-70 Kbps	20-30 Kbps
在面板上切换选项卡	40-50 Kbps	20-50 Kbps	10-20 Kbps
关闭面板	50-100 Kbps	40-60 Kbps	20-30 Kbps
更改面板选项	2-10 Kbps	1-5 Kbps	1-3 Kbps
打开浏览器页面	100-300 Kbps	50-200 Kbps	40-80 Kbps
滚动浏览器	75-200 Kbps	50-200 Kbps	30-100 Kbps
关闭浏览器	100-150 Kbps	75-100 Kbps	30-60 Kbps
打开开始菜单	75-100 Kbps	50-75 Kbps	20-30 Kbps
关闭开始菜单	75-100 Kbps	25-50 Kbps	10-15 Kbps
星空屏幕保护	25-50 Kbps	10-15 Kbps	7-10 Kbps
3D 管道屏幕保护	10-100 Kbps	5-20 Kbps	2-10 Kbps
Windows 媒体视频	500-1200 Kbps	300-500 Kbps	150-300 Kbps
QuickTime 视频 1	700-2500 Kbps	400-500 Kbps	150-350 Kbps
QuickTime 视频 2	1500-2500 Kbps	400-550 Kbps	200-350 Kbps

如果降低带宽设置，实际上可以大大降低所有任务使用的带宽。如果使用 15 位彩色设置，视觉效果类似默认参数。此外，更改其他设置也可以降低带宽。

请注意这些带宽数字仅供参考，由于存在许多因素，在不同的环境下看到的效果可能会有所不同。

如果减小带宽？

Dominion KX II 远程客户机有许多设置，可以优化带宽和性能。在标准 LAN/WAN 环境下，默认设置具有机架访问级性能，带宽用量较小。

带宽管理设置包括连接速度和颜色深度。降低带宽：

降低连接速度

降低连接速度可以大大降低带宽用量。在标准 LAN/WAN 环境下，将连接速度设置为 1.5Mbps 或 1Mbps，在保持良好性能的情况下降低带宽。进一步降低设置可以进一步降低带宽，适用于低带宽链路。

降低颜色深度

降低颜色深度也可以大大降低带宽并提高性能，但使用的颜色较少，可能会使视频质量下降。对某些管理任务而言，这是可以接受的。

对于低速 Internet 连接，使用 8 位颜色或更小的颜色深度可以降低带宽，提高性能。

可降低带宽的其他措施包括：

- 使用单色桌面背景，而不使用复杂图像。
- 禁用屏幕保护
- 在目标服务器上使用较低的分辨率
- 取消 Windows 的 Show window contents while dragging（在拖动窗口时显示窗口内容）选项
- 使用简单图像、主题和桌面（例如 Windows Classic）。

如果带宽链路速度较低，我该怎么办？

可以调节连接速度设置和颜色深度设置，从而优化低带宽链路的性能。例如在 Multi-Platform Client 或 Virtual KVM Client 上将连接速度设置为 1.5Mbps 或 1Mbps，将颜色深度设置为 8 位。在带宽非常小的情况下，甚至可以使用更小的连接速度和颜色深度。

我想通过 Internet 联网。联网性能如何？



取决于远程客户机和 Dominion KX II 之间的 Internet 连接的带宽和延迟时间。在使用电缆调制解调器或高速 DSL 连接时，性能与 LAN/WAN 连接相仿。在使用低速链路时，采用上述建议提高性能。

我的网络环境有很高的带宽。如何优化性能？

在大带宽环境下，默认设置具有很好的性能。确保将连接速度设置为 100Mbps 或 1Gbps，将颜色深度设置为 15 位 RGB 彩色。

最高支持多高的远程 (IP) 视频分辨率？

Dominion KX II 是首款也是唯一一款 KVM-over-IP 切换器，支持全高清晰度远程视频分辨率 1920x1080。

此外，还支持包括 1600x1200、1680x1050 和 1440x900 在内的宽屏格式，所以远程用户可以使用目前的高分辨率监视器。

配备 DVI 端口的服务器有何优点？

配备同时支持 DVI-A（模拟）和 DVI-I（集成模拟和数字）的 DVI 端口的服务器，可以利用 ADVI-VGA 等简单的无源适配器把 DVI 端口转换成 VGA 插头，从而连接 Dominion KX II CIM 的 VGA 插头。

配备只支持 DVI-D（数字）的 DVI 端口的服务器，可能要使用较贵的适配器，但客户应该检查服务器显示卡配置是支持 DVI-I 还是 DVI-A。

Ethernet 和 IP 联网

Dominion KX II 是否有双 Gigabit Ethernet 端口实现冗余故障切换？

是。Dominion KX II 有双 Gigabit Ethernet 端口，具备冗余故障切换能力。如果主 Ethernet 端口（或相连的交换机/路由器）发生故障，Dominion KX II 切换到备用网络端口（使用同一个 IP 地址），确保服务器工作不中断。注意：管理员必须启用自动故障切换。

Dominion KX II 的 Ethernet 接口速度有多大？

Dominion KX II 支持 Gigabit 和 10/100Mbps Ethernet。Dominion KX II 支持两个 10/100/1000Mbps Ethernet 接口，速度设置和双工设置可以配置（自动检测或人工设置）。

Dominion KX II 是否有双 Gigabit Ethernet 端口实现冗余故障切换或负载平衡？

是。Dominion KX II 配有双千兆以太网端口，以提供冗余故障切换功能。如果主以太网端口（或者与它相连的交换机/路由器）发生故障，Dominion KX II 将故障切换到具有相同 IP 地址的备用网络端口，确保服务器操作不中断。注意：管理员必须启用自动故障切换。

是否可以通过无线连接访问 Dominion KX II？

是。Dominion KX II 只使用标准 Ethernet 和少量带宽，提供高质量视频。因此，如果无线客户机与 Dominion KX II 之间有网络连接，可以采用无线方式在 BIOS 级配置和管理服务器。

是否可以通过 WAN (Internet) 使用 Dominion KX II，还是只能在公司 LAN 内部使用它？

无论采用快速公司 LAN、很难预测的 WAN (Internet)、电缆调制解调器还是拔号调制解调器，Dominion KX II 的 KVM-over-IP 技术均可支持相应的连接。

是否可以用 VPN 访问 Dominion KX II？

是，Dominion KX II 在第一层到第四层使用标准的 Internet Protocol (IP) 技术，很容易采用 VPN 技术通过隧道发送流量。

是否可以同时使用 Dominion KX II 和代理服务器？

是。Dominion KX II 只能与 SOCKS 代理服务器一起使用，假设远程客户机 PC 配置正确。阅读用户手册或联机帮助了解详情。

为了启用 Dominion KX II 网络访问，必须在防火墙上打开多少 TCP 端口？这些端口是否可以配置？



只需打开一个端口。Dominion KX II 只需访问一个 TCP 端口，从而保护网络安全。此端口可以配置，可以进一步增强网络安全。

当然要注意的是，如要使用 Dominion KX II 的可选网络浏览器功能，还必须打开标准的 HTTPS 端口 443。

Dominion KX II 是否使用外部验证服务器？

不，Dominion KX II 是自给自足的。在给 Dominion KX II 分配 IP 地址之后，就可以使用它了。它的网络浏览器和验证功能全部是内置的。

如果使用外部验证服务器（例如 LDAP、Active Directory、RADIUS 等），Dominion KX II 也允许这么做，甚至可以在外部验证服务器不可用时，切换到自己的内置验证。这样可以优化 Dominion KX II 的设计理念，更容易安装，与外部验证服务器没有任何关系，灵活性最大。

Dominion KX II 是否支持 CITRIX？

可以适当配置 Dominion KX II 支持 CITRIX 等远程访问产品，但 Raritan 不能保证其性能是可接受的。CITRIX 等产品使用的视频重定向技术在概念上类似数字化 KVM 切换器，所以可以同时使用这两种 KVM-over-IP 技术。

Dominion KX II 是否可以使用 DHCP？

可以使用 DHCP 寻址模式，但 Raritan 建议你使用固定地址，因为 Dominion KX II 是基础设施设备，使用固定 IP 地址可以更高效地访问和管理它。

我在通过公司 IP 网络连接 Dominion KX II 时出问题。这很可能是什么问题？

Dominion KX II 依赖 LAN/WAN 网络。可能会发生这些问题：

- Ethernet 自动协商 — 在某些网络上，10/100 自动协商不能正常工作，必须将 Dominion KX II 设备设置为 100MB/全双工，或者选择网络要求的设置。
- IP 地址重复 — 如果 Dominion KX II 的 IP 与另一台设备的 IP 地址相同，网络连接可能会出现不一致现象。
- 端口 5000 冲突 — 如果另一台设备使用端口 5000，必须更改 Dominion KX II 默认端口，或者更改另一台设备的端口。

在更改 Dominion KX II 的 IP 地址或更换新的 Dominion KX II 时，必须让第二层网络和第三层网络了解其 IP 地址和 MAC 地址，这需要足够的时间。



IPv6 联网

什么是 IPv6？

IPv6 是 Internet Protocol Version 6 的缩写。IPv6 是下一代 IP 协议，将取代目前使用的 IP Version 4 (IPv4) 协议。

IPv6 解决了 IPv4 存在的许多问题，例如 IPv4 地址数很有限。它还在路由和网络自动配置等方面较 IPv4 有了重大改进。IPv6 有望逐步取代 IPv4，在未来数年内将出现二者共存局面。

从管理员角度看，IPv6 解决了 IP 网络最头痛的一个问题，那就是 IP 网络配置和管理。

为什么 Dominion KX II 支持 IPv6 联网？

美国政府各部门和国防部规定现在必须购买与 IPv6 兼容的产品。此外，许多企业和国家（例如中国）将在未来几年内过渡到 IPv6。

双协议堆是什么？为什么需要它？

双协议堆就是可同时支持 IPv4 协议和 IPv6 协议。由于要逐步从 IPv4 过渡到 IPv6，所以双协议堆是 IPv6 支持的基本要求。

如何在 Dominion KX II 上启用 IPv6？

利用 Dominion KX II 的 Device Settings（设备设置）菜单打开 Network Settings（网络设置）页。启用 IPv6 寻址模式，选择人工或自动配置。还必须在 MPC 上启用它。

如果要使用的外部服务器使用 IPv6 地址，使用 Dominion KX II 时会发生什么情况？

Dominion KX II 可以通过外部服务器的 IPv6 地址访问这些服务器，例如 SNMP 管理器、系统日志服务器或 LDAP 服务器。

可以利用 Dominion KX II 的双协议堆体系结构，通过 (1) IPv4 地址、(2) IPv6 地址或 (3) 主机名访问这些外部服务器。所以，Dominion KX II 支持许多客户的 IPv4/IPv6 混合环境。

Dominion KX I 是否支持 IPv6？

不，Dominion KX I 不支持 IPv6 地址。

如果网络不支持 IPv6，会发生什么情况？

在出厂时，Dominion KX II 默认联网协议设置为纯 IPv4。如果准备使用 IPv6，要根据上述说明启用 IPv6/IPv4 双协议堆。

可以在哪里进一步了解 IPv6？



可以在 www.ipv6.org 上了解 IPv6。Dominion KX II 用户指南说明 Dominion KX II 对 IPv6 的支持。

服务器

Dominion KX II 是否依赖 Windows 服务器？

绝对不依赖 Windows 服务器。由于用户使用可在任何情况下使用的 KVM 基础设施（他们可能必须用 KVM 基础设施解决问题），所以 Dominion KX II 与任何外部服务器没有任何关系。例如假如数据中心受到恶意 Windows 蠕虫或病毒的攻击，管理员必须用 KVM 解决方案解决问题。因此，KVM 解决方案不必依赖这些 Windows 服务器（或其他服务器），照样能正常工作。

因此，Dominion KX II 是完全独立的设备。即使用户配置 Dominion KX II 用 Active Directory 服务器进行验证，假如 Active Directory 服务器不可用，就激活并使用 Dominion KX II 自己的验证机制。

为了使用 Dominion KX II 的网络浏览器功能，是否必须安装 Microsoft® Internet Information Services (IIS) 等 Web 服务器？

不，Dominion KX II 是自给自足的设备。在给 Dominion KX II 分配 IP 地址之后，就可以使用它了，因为它在内部集成了网络浏览器和验证能力。

为了在特定工作站上访问 Dominion KX II，必须安装什么软件？

不用安装任何软件。Dominion KX II 可以通过网络浏览器访问。但 Raritan 网站 (www.raritan.com) 提供可选安装的客户机，调制解调器连接需要此客户机。基于 Java 的客户机现在可供非 Windows 用户使用。

需要如何配置服务器，才能连接 Dominion KX II？

只需设置鼠标参数让用户在远程连接过程中实现最佳鼠标同步，同时关闭那些会影响屏幕显示的电源管理功能。但如果使用新的 D2CIM-VUSB 适配器（支持绝对鼠标同步），不必人工设置鼠标参数。

鼠标同步怎么样？

对很多 KVM-over-IP 用户来说，鼠标同步是一件很麻烦的事情。Dominion KX II 绝对鼠标同步功能使鼠标完全同步，不需要在 Windows 和 Apple® Mac® 服务器上更改服务器鼠标设置。对于其他服务器，可以使用智能鼠标模式或快速单鼠标模式避免更改服务器鼠标设置。

刀片服务器

是否可以将刀片服务器连接到 Dominion KX II？

可以。Dominion KX II 支持下列主要刀片服务器制造商推出的常用刀片服务器产品：HP®、IBM® 和 Dell®。

支持哪些刀片服务器？

支持下列产品：

- Dell® PowerEdge® 1855, 1955 and M1000e
- HP BladeSystem c3000 和 c7000
- IBM® BladeCenter® H and E

注意：IBM BladeCenter Model S、T 和 HT 用 IBM（其他）选项处理。



是否使用 **Paragon** 刀片服务器 **CIM**？

不行，Dominion KX II 无法使用 Paragon II 的刀片服务器 CIM。

应该使用哪种 **CIM**？

取决于你使用的特定型号刀片服务器的 KVM 端口的类型。支持下列 CIM：DCIM-PS2、DCIM-USBG2、D2CIM-VUSB 和 D2CIM-DVUSB。

可以使用哪些访问和控制？

Dominion KX II 提供自动化安全 KVM 访问：(1) 在机架上访问，(2) 基于 IP 的远程访问，(3) 通过 CommandCenter 访问，(4) 通过调制解调器访问。

是否必须用键盘在不同的刀片服务器之间来回切换？

某些刀片服务器要求你用热键在不同的刀片服务器之间来回切换。在使用 Dominion KX II 时，不必使用这些热键。只需单击刀片服务器名称，Dominion KX II 就自动切换到该刀片服务器，不需要使用热键。

是否可以访问刀片服务器管理模块？

是，可以定义管理模块 URL，在 Dominion KX II 或 CC-SG 上访问它。如果这样配置，只需单击一下即可访问管理模块。

一台 **Dominion KX II** 可以连接多少刀片服务器？

为了保证性能和可靠性，最多可以将八个任何型号的刀片服务器机箱连接到一台 Dominion KX II。Raritan 建议你将设备支持的远程连接数加倍。例如对于有两个远程通道的 KX2-216，我们建议你最多连接四个刀片服务器机箱。当然，可以将各台服务器连接到其余服务器端口。

我们是使用几台 **Dominion KX II** 的中小企业，是否必须使用 **CC-SG** 管理工作站？

不，不必这样做。中小企业客户不用 CC-SG，也能使用新刀片服务器功能。

I'm an enterprise customer using CC-SG.是否可以通过 **CC-SG** 访问刀片服务器？

是。在 Dominion KX II 上配置刀片服务器之后，CC-SG 用户可以通过 KVM 连接访问这些服务器。此外，刀片服务器按机箱和 CC-SG 定制视图进行组织管理。

如果使用带内 **KVM** 访问或嵌入式 **KVM** 访问，会发什么情况？

是，可以在 CC-SG 上配置刀片服务器带内访问和嵌入式访问。

I'm running VMWare on some of my blade servers.是否支持它？

是，在使用 CC-SG 时，可以显示和访问在刀片服务器上运行的虚拟机。



是否支持虚拟媒体？

IBM BladeCenter® H 型和 E 型（安装 D2CIM - DVUSB）支持虚拟媒体。

是否支持绝对鼠标同步？

在刀片服务器机箱上安装了内置 KVM 切换器的服务器，通常不支持绝对鼠标技术。对于 HP 刀片服务器和部分 Dell 刀片服务器，每个刀片服务器连接一个 CIM，只要在刀片服务器上运行基本操作系统，就支持绝对鼠标。

刀片服务器访问是否安全？

是，刀片服务器访问使用所有标准的 Dominion KX II 安全功能，例如 128 位或 256 位加密。此外，还有刀片服务器特定的安全功能，例如刀片服务器访问权限和热键锁定，防止未经授权的访问。

Dominion KSX II 或 KX II-101 是否支持刀片服务器？

这些产品现在还没有这些新刀片服务器功能。



安装

除了 Dominion KX II 设备本身，安装它还需要向 Raritan 订购什么？

与 Dominion KX II 相连的每台服务器需要一个 Dominion 或 Paragon 计算机接口模块 (CIM)，用于直接连接服务器的键盘端口、视频端口和鼠标端口。

应该在安装时使用哪种五类电缆？

Dominion KX II 可以使用任何标准 UTP（非屏蔽双绞线）电缆：5 类、5e 类或 6 类。在 Raritan 的手册和销售材料上，我们统称这些电缆为五类电缆。实际上可以用任何品牌的 UTP 电缆连接 Dominion KX II。

可以将哪几种服务器连接到 Dominion KX II？

Dominion KX II 与服务器供应商无关。只要服务器配备标准键盘端口、视频端口和鼠标端口，都可以连接到 Dominion KX II。

如何将服务器连接到 Dominion KX II？

与 Dominion KX II 相连的服务器需要一个 Dominion CIM 或 Paragon CIM，用于直接连接服务器的键盘端口、视频端口和鼠标端口。然后用 5 类、5e 类或 6 类等标准 UTP（双绞线）电缆将每个 CIM 连接到 Dominion KX II。

服务器可以距离 Dominion KX II 多远？

一般地，服务器最多可以距离 Dominion KX II 150 英尺 (45m) 远，视服务器类型而定。浏览 Raritan 网站 (www.raritan.com) 或参看***目标服务器连接距离和视频分辨率*** (p. 267)了解详情。对于支持虚拟媒体和绝对鼠标同步的新的 D2CIM-VUSB 和 D2CIM-DVUSB CIM，建议距离不要超过 100 英尺 (30m)。

在工作过程中断开键盘或鼠标时，某些操作系统会锁住。在断开与 Dominion KX II 相连的服务器时，什么东西可以防止服务器锁住？

每个 Dominion 计算机接口模块 (DCIM) dongle 给相连的服务器充当虚拟键盘和虚拟鼠标。这种技术称为 KME (keyboard/mouse emulation)。Raritan 的 KME 技术是数据中心级的，经过实践检验，其可靠性远远超过低端 KVM 切换器使用的技术：这是十五年开发经验的结晶，已在全球应用于数百万台服务器。

是否必须在与 Dominion KX II 相连的服务器上安装任何代理？

与 Dominion KX II 相连的服务器不需要安装任何软件代理，因为 Dominion KX II 通过硬件直接连接服务器的键盘端口、视频端口和鼠标端口。

每台 Dominion KX II 设备可以连接多少台服务器？

Dominion KX II 产品的 1U 机箱有 8 个、16 个或 32 个服务器端口，2U 机箱有 64 个服务器端口。数字 KVM 切换器端口密度是业界最高的。

如果将一台服务器与一台 Dominion KX II 设备断开，将它重新连接到另一台 Dominion KX II 设备，或者将它连接到同一台 Dominion KX II 设备的不同端口，会发生什么情况？

当服务器从一个端口移动到另一个端口时，Dominion KX II 自动更新服务器端口名称。此外，这种自动更新不能影响本地访问端口，而且还广播到所有远程客户机和可选的 CommandCenter Secure Gateway 管理工具。

如何将 Cisco 路由器/交换机或 Sun™ 无头服务器等串行控制 (RS-232) 设备连接到 Dominion KX II？

如果只有几台串行控制设备，可以用新的 Raritan P2CIM-SER 串行转换器将它们连接到 Dominion KX II。

但如果有四台以上串行控制设备，我们建议你使用 Raritan KSX II 系列或 SX 系列安全控制台服务器。这些设备很容易使用、配置和管理，可与 Dominion 系列产品完全集成在一起。许多 UNIX 管理员和联网管理员特别欣赏 SSH 和设备的直接连接能力。



本地端口

如何将多台 Dominion KX II 设备连接起来构成一个解决方案？

是否可以在机架上直接访问服务器？

是。在机架上，Dominion KX II 很像传统的 KVM 切换器，可以通过一套键盘、监视器和鼠标，最多对 64 台服务器进行控制。

是否可以合并多台 Dominion KX II 产品的本地端口？

是。可以利用 Dominion KX II 的级联功能，把多台 Dominion KX II 切换器的本地端口连接到另一台 Dominion KX II。然后可以在数据中心的一个点，通过合并端口列表访问与 Dominion KX II 设备相连的这些服务器。

在使用本地端口时，是否妨碍其他用户远程访问服务器？

不。Dominion KX II 本地端口提供完全独立的服务器访问路径。这意味着用户可以在机架上本地访问服务器，不影响同时远程访问机架的用户数。

是否可以在本地端口上使用 USB 键盘或鼠标？

是。Dominion KX II 本地端口提供 PS/2 和 USB 两种形式的键盘端口和鼠标端口。注意 USB 端口是 USB v1.1，只支持键盘和鼠标，不支持扫描仪或打印机等 USB 设备。

在机架上是否有显示屏进行本地访问？

是，但 Dominion KX II 的机架访问超出了传统的显示屏。Dominion KX II 有业界第一个机架访问浏览器界面，其本地端口用同一个界面进行本地访问和远程访问。此外，大多数管理功能可以在机架上执行。

在使用本地端口时，如何选择不同的服务器？

本地端口采用与远程客户机相同的用户界面显示相连的服务器。只需单击一下鼠标即可连接服务器。

如何确保只有授权用户可以通过本地端口访问服务器？

尝试使用本地端口的用户必须进行与远程访问相同的验证。这意味着：

- 如果配置 Dominion KX II 与外部 RADIUS、LDAP 或 Active Directory 服务器交互操作，尝试使用本地端口的用户也用相同的服务器进行验证。
- 如果外部服务器不可用，Dominion KX II 切换到自己的内部验证数据库。
- Dominion KX II 有自己的独立验证机制，便于立刻进行整体安装。

如果用本地端口更改相连服务器的名称，此更改是否广播到远程访问客户机？它是否广播到可选的 CommandCenter 设备？

是。本地端口显示与远程访问客户机和可选的 Raritan CommandCenter Secure Gateway 管理设备相同，且保持完全同步。需要说明的是，如果更改 Dominion KX II 屏幕显示的服务器名称，将实时更新所有远程客户机和外部管理服务器。

如果用 Dominion KX II 的远程管理工具更改相连服务器的名称，此更改是否广播到本地端口显示屏？

是。如果远程更改服务器名称，或者通过可选的 Raritan CommandCenter Secure Gateway 管理设备更改服务器名称，立刻影响 Dominion KX II 的显示屏。

有时我看到本地端口用户界面上有阴影。为什么会出现这种现象？

这种阴影/幻影效果可能是 LCD 监视器通电时间过长造成的。如果 LCD 屏幕通电时间过长，LCD 本身的特性和电荷/静电荷会产生这些效果。



扩展本地端口（仅 Dominion KX2-832 和 KX2-864 型）

什么是扩展本地端口？

Dominion KX2-832 和 KX2-864 具备扩展本地端口。Dominion KX II 八用户型有一个标准本地端口和一个新的扩展本地端口，可以利用五类电缆把扩展本地端口连接到机架之外的控制室、数据中心的另一个点或 Paragon II 切换器。

是否可以将扩展本地端口连接到 Dominion KX II？

是，可以利用 Dominion KX II 的级联功能，把扩展本地端口连接到另一台 Dominion KX II 的服务器端口。

扩展本地端口是否需要用户工作站？

是，下列设备可以给扩展本地端口充当用户工作站：Paragon II EUST、Paragon II UST 和 Cat5 Reach URKVMG 设备。此外，可以用五类电缆把扩展本地端口连接到 Paragon II 切换器的服务器端口。可以用此配置把许多 KX2-8xxx 设备的本地端口整合到一台切换器上。

用户工作站可以距离 Dominion KX II 多远？

距离在 200-1000 英尺之间，但随用户工作站类型、视频分辨率、电缆类型和质量而变。

是否需要 CIM？

不需要 CIM。只需连接一根五类电缆。

我必须使用扩展本地端口吗？

不，扩展本地端口是可选端口，默认禁用此端口。在 Local Port Settings（本地端口设置）页上启用它。为安全起见，如果不使用标准本地端口，也可以禁用此端口。



电源控制

Dominion KX II 是否有双电源？

所有 Dominion KX II 产品均配备双交流输入和双电源，支持自动故障切换。如果其中一个电源输入或电源发生故障，Dominion KX II 自动切换到另一个电源输入或电源。

Dominion KX II 使用的电源是否自动检测电压设置？

是。Dominion KX II 电源可以使用的交流电压是 100-240 伏，频率是 50-60Hz。

如果电源或电源输入发生故障，是否通知我？

Dominion KX II 面板上的 LED 指示灯告知用户电源发生故障。也可以在审计日志里增加一项，并在 Dominion KX II Remote Client 用户界面上显示出来。如果管理员这样配置电源，将生成 SNMP 事件或系统日志事件。

Dominion KX II 有哪些电源控制功能？

可以将 Raritan 远程电源控制电源条连接到 Dominion KX II 上，以便控制 KVM 目标服务器的电源。在简单的一次性配置之后，只需用右键单击服务器名称，即可给服务器通电、断电或重新通电。注意硬启动相当于拔下服务器的交流电源插头，然后再插上插头。

一台 Dominion KX II 可以连接多少 PDU？

每台 Dominion KX II 设备最多可以连接八个 PDU。

如何将 PDU 连接到 Dominion KX II？

用 D2CIM-PWR 把电源条连接到 Dominion KX II。必须单独购买 D2CIM-PWR，PDU 不带 D2CIM-PWR。

Dominion KX II 是否支持有多个电源的服务器？如果每个电源连接不同的电源条，会发生什么情况？

是。很容易配置 Dominion KX II 支持与多个电源条相连的多个电源。每台 Dominion KX II 设备最多可以连接八个电源条。可以将每台目标服务器的四个电源连接到多个电源条。

Dominion KX II 是否显示 PDU 统计数据和测量数据？

是。检索 PDU 级电源统计数据并给用户显示这些数据，包括功率、电流和电压。

远程电源控制是否要求任何特殊服务器配置？



某些服务器配备默认 BIOS 设置，使服务器在掉电并重新通电之后不自动重新启动。对于这些服务器，参看相应的服务器说明书更改此设置。

在给服务器重新通电时，会发生什么后果？

这实际上相当于拔下服务器的交流电源插头，然后再插上插头。

是否可以接通/断开与一个 PDU 相连的其他设备（非服务器）？

是。可以通过 Dominion KX II 的浏览器界面，按电源接口接通/断开与 PDU 相连的其他设备的电源。

Dominion KX II 支持哪几种电源条？

为了利用 Dominion KX II 的集成电源控制用户界面，更重要的是利用其集成安全，要使用 Raritan 远程电源控制 (RPC) 电源条。RPC 配有许多电源接口、连接器和电流额定值。如要将 RPC 连接到 Dominion KX II，必须购买 D2CIM-PWR。

伸缩性

如何将多台 Dominion KX II 设备连接起来构成一个解决方案？

如要把多台 Dominion KX II 设备连起来形成合并本地访问，可以利用 Dominion KX II 的级联功能把多层（级联）Dominion KX II 切换器的本地端口连接到基础 Dominion KX II。然后可以在数据中心的一个点，通过合并端口列表访问与 Dominion KX II 设备相连的这些服务器。

必须用 D2CIM-DVUSB CIM 把级联 Dominion KX II 切换器连接到基础切换器。对于 KX2-832 和 KX2-864，可以用五类/六类电缆把扩展本地端口连接到基础 Dominion KX II 切换器（不需要 CIM）。

可以在数据中心甚至远程 PC 上通过合并端口列表进行访问。可以通过分层端口列表或采用搜索方式(使用通配符）,访问与级联 Dominion KX II 相连的所有服务器。

支持两层；在级联配置里，最多可以访问 1024 台设备。还支持远程电源控制。

未来版本将支持通过级联访问方式访问虚拟媒体、智能卡和刀片服务器。当然，只有在通过标准远程连接进行访问时，才能使用这些功能。

虽然通过合并端口列表访问远程 IP 服务器很方便，但为了实现最佳性能，建议你在 CommandCenter 上或服务器直接连接的 Dominion KX II 上访问级联服务器。

如何将 Dominion KX II 设备连起来？

多台 Dominion KX II 设备之间不必有物理连接。每台 Dominion KX II 设备连接网络，如果使用 Raritan CommandCenter Secure Gateway (CC-SG) 管理设备，它们将自动作为一个解决方案一起工作。

CC-SG 给远程访问和管理充当一个接入点。CC-SG 有许多便捷工具，例如综合配置数据库、综合固件更新数据库、单一验证和授权数据库。

用 CC-SG 集中管理远程访问的客户可以充分利用 Dominion KX II 的级联（级联）功能把多台 Dominion KX II 切换器的本地端口组合在一起，在数据中心的一个控制台上最多可以本地访问 1024 台服务器。

是否需求 CC-SG？

对于想单独使用（不使用中央管理系统）的客户，多台 Dominion KX II 设备仍然能通过 IP 网络实现互操作，可以伸缩。可以在 Dominion KX II web 用户界面或 Multiplatform Client (MPC) 上访问多台 Dominion KX II。

是否可以将现有的模拟 KVM 切换器连接到 Dominion KX II？



是。可以将模拟 KVM 切换器连接到其中一台 Dominion KX II 的服务器端口。只需使用一个 D2CIM-DVUSB 或 D2CIM-VUSB，把它插入现有的模拟 KVM 切换器的用户端口。请注意模拟 KVM 切换器的规格变化很大，Raritan 不能保证第三方的特殊模拟 KVM 切换器可以互操作。联系 Raritan 技术支持部门了解详情。

计算机接口模块 (CIM)

Raritan 模拟阵列 KVM 切换器 Paragon 计算机接口模块 (CIM) 是否可与 Dominion KX II 一起使用？

是。某些 Paragon 计算机接口模块 (CIM) 可与 Dominion KX II 一起使用（浏览网站上的 Raritan Dominion KX II 版本说明，了解最新认证的 CIM 清单）。

但由于 Paragon CIM 比 Dominion KX II CIM 贵得多(因为它们集成了高达 1000 英尺 [300m] 的视频传输技术），建议你一般不要购买 Paragon CIM 与 Dominion KX II 一起使用。还要注意在连接 Dominion KX II 时，Paragon CIM 的最大视频传输距离为 150 英尺，与 Dominion KX II CIM 相同，而不是连接 Paragon 时的 1000 英尺 [300m]。

Dominion KX II 计算机接口模块 (CIM) 是否可与 Raritan 模拟阵列 KVM 切换器 Paragon 一起使用？

不。Dominion KX II 计算机接口模块 (CIM) 的视频传输距离为 50-150 英尺 (15-45m)，所以不能与 Paragon 一起使用，后者要求 CIM 的视频传输距离为 1000 英尺 (300m)。为了确保 Raritan 的所有客户获得业界最高质量的视频（这是 Raritan 的宗旨），Dominion 系列 CIM 不能与 Paragon 互操作。

Dominion KX II 是否支持 Paragon Dual CIM？

是。Dominion KX II 现在支持 Paragon II Dual CIM（P2CIM-APS2DUAL 和 P2CIM-AUSBDUAL），可以把数据中心的两台服务器连接到两台不同的 Dominion KX II 切换器。

如果一台 Dominion KX II 切换器不可用，可以通过第二台 Dominion KX II 切换器访问服务器，从而实现冗余访问，使远程 KVM 访问权加倍。

请注意这些 CIM 是 Paragon CIM，所以它们不支持 Dominion KX II 高级功能，例如虚拟媒体和绝对鼠标等。

安全

Dominion KX II 是否经过 FIPS 140-2 认证？

Dominion KX II 作为 2.2.0 版本的一部分，使用户能使用在 Linux 平台上运行的嵌入式 FIPS 140-2 认证加密模块，按 FIPS 140-2 实现指导原则进行加密。用此加密模块加密 KVM 会话流量，包括视频数据、键盘数据、鼠标数据、虚拟媒体数据和智能卡数据。

Dominion KX II 使用哪种加密方法？

Dominion KX II 使用业界标准的（最安全的）RC4 或 AES 加密方法，两种方法都采用 SSL 通信及其数据流。在远程客户机和 Dominion KX II 之间传输的所有数据都经过加密。

Dominion KX II 是否支持美国政府 NIST 的 FIPS 标准建议的 AES 加密方法？

Dominion KX II 使用 Advanced Encryption Standard (AES) 加密方法增强安全。

AES 是美国政府批准的加密算法，是 National Institute of Standards and Technology (NIST) 的 FIPS Standard 197 建议的算法。

Dominion KX II 是否加密视频数据？还是只加密键盘数据和鼠标数据？

与竞争对手采用的仅加密键盘数据和鼠标数据解决方案不同的是，Dominion KX II 同时加密键盘数据、鼠标数据和视频数据，从而增强安全。

Dominion KX II 如何与 Active Directory®、RADIUS 或 LDAP 等外部验证服务器集成在一起？

可以通过很简单的配置，将 Dominion KX II 设置为将所有验证请求转发到 LDAP、Active Directory 或 RADIUS 等外部服务器。对于每个已验证的用户，Dominion KX II 接收来自验证服务器的、该用户所属的用户组。Dominion KX II 然后根据用户所属的用户组，确定他/她的访问权。

如何存储用户名和密码？

如果使用 Dominion KX II 的内部验证功能，采用加密格式存储用户名和密码等所有敏感信息。任何人都无法获取这些用户名和密码，包括 Raritan 技术支持部或产品开发部。

Dominion KX II 是否支持强密码？

是，Dominion KX II 有管理员可配置的强密码检查机制，确保用户创建的密码符合公司标准和/或政府标准的规定，可以防止恶意破解。

如果 Dominion KX II 加密模式设置为自动，可以实现哪一级加密？



自动协商加密等级取决于所用的浏览器。

是否可以将自己的数字证书上载到 Dominion KX II？

是。客户可以把自签名证书或证书机构提供的数字证书上载到 Dominion KX II 上增强验证和安全通信。

Dominion KX II 是否支持可配置的安全提示？

是。对于在用户登录前需要安全消息的政府机构、军队和其他对安全要求很高的客户，Dominion KX II 可以显示用户可配置的提示消息，可以有选择地要求用户接受安全协议。

我的安全策略不允许使用标准 TCP 端口号。如何更改端口号？

是。对于要避免使用标准 TCP/IP 端口号并增强安全的客户，Dominion KX II 允许管理员配置替代端口号。



智能卡和 CAC 验证

Dominion KX II 是否支持智能卡验证和 CAC 验证？

是，2.1.10 和更高版本支持对目标服务器进行智能卡和 DoD Common Access Card (CAC) 验证。

哪些 Dominion KX II 型号支持智能卡/CAC？

所有 Dominion KX II 型号都支持智能卡/CAC。Dominion KSX2 和 KX2-101 目前不支持智能卡和 CAC。

大企业客户和中小企业客户是否也使用智能卡？

是。最大胆的智能卡部署客户是美国联邦政府。

哪些 CIM 支持智能卡/CAC？

需要使用 D2CIM-DVUSB。必须把此 CIM 的固件升级到 2.1.10 版本和更高版本的固件。

需要哪个固件版本？

需要 Dominion KX II 2.1.10 和更高版本。

支持哪些智能卡读卡器？

所需的读卡器标准是 USB CCID 和 PC/SC。参看 Dominion KX II 2.1.10 *支持的和不支持的智能卡读卡器* (p. 270)或版本说明，了解认证的读卡器清单和其他信息。

能否在本地端口上通过 Command Center 进行智能卡/CAC 验证？

是。为了使用本地端口，把兼容的智能卡读卡器连接到 Dominion KX II 的 USB 端口。

是否使用支持 Paragon 智能卡的 UST 和 CIM？

不，P2-EUST/C 和 P2CIM-AUSB-C 不是 Dominion KX II 解决方案的一部分。



可管理性

是否可以通过网络浏览器远程管理和配置 Dominion KX II？

是，完全可以通过网络浏览器配置 Dominion KX II。注意这不要求你在工作站上安装适当版本的 Java Runtime Environment (JRE)。

除了首次设置 Dominion KX II IP 地址，可以通过网络设置该解决方案的所有设置。（实际上，如果使用 Ethernet 交叉电缆和 Dominion KX II 默认 IP 地址，甚至可以通过网络浏览器配置首次设置。）

是否可以备份和恢复 Dominion KX II 的配置？

是，可以备份 Dominion KX II 设备配置和用户配置，以便在发生灾难时供恢复之用。

可以通过网络或远程控制台，远程使用 Dominion KX II 的备份和恢复功能。

Dominion KX II 提供哪种审计或日志？

为便于追踪，Dominion KX II 记录所有重大用户事件和系统事件，有日期和时间戳。例如报告的事件包括（但不仅限于）：用户登录、用户退出、用户访问特定服务器、登录失败、配置更改等。

Dominion KX II 是否可以集成系统日志？

是。除了 Dominion KX II 自己内部的日志功能，Dominion KX II 还可以将所有日志事件发送到中央系统日志服务器。

Dominion KX II 是否可以集成 SNMP？

是。除了 Dominion KX II 自己内部的日志功能，Dominion KX II 还可以将 SNMP 陷阱发送到 HP Openview 和 Raritan CC-NOC 等 SNMP 管理系统。

Dominion KX II 的内部时钟是否可与时间服务器同步？

是，Dominion KX II 支持业界标准的 NTP 协议，可与公司的时间服务器或任何公共时间服务器同步（假定公司防火墙允许出站 NTP 请求）。

其他

Dominion KX II 默认 IP 地址是什么？

192.168.0.192

Dominion KX II 默认用户名和密码是什么？

Dominion KX II 默认用户名是 admin，默认密码是 raritan（全部小写）。但为了最大限度地增强安全，Dominion KX II 强制管理员在首次启动 Dominion KX II 时更改默认管理用户名和密码。

我更改了 Dominion KX II 管理密码，后来忘了密码，你是否能替我找回密码？

Dominion KX II 有一个硬件复位按钮，可以用它将设备的管理密码复位到出厂设置。

我用 Firefox® 登录 Dominion KX II，打开另一个 Firefox 浏览器窗口。第二个 Firefox 浏览器窗口自动登录同一台 Dominion KX II。这样做是否正确？

是，这是正常现象，是浏览器和 cookies 直接发挥作用的结果。

我用 Firefox 登录 Dominion KX II，尝试在同一个客户机上用另一个 Firefox 浏览器会话登录另一台 Dominion KX II，结果却从两台 Dominion KX II 上退出来。这是否是正常现象？

是。如要访问两台不同的 Dominion KX II 设备，要么关闭第一个会话，要么使用另一台客户机 PC。

在用 Firefox 浏览器运行 KVM 会话时，Virtual KVM Client 自动打开某些对话框（例如 Connection Properties [连接属性]和 Video Settings [视频设置]），似乎封锁了 Firefox 浏览器（甚至包括其他 Firefox 会话）。我该怎么办？

这是正常现象，因为所有 Firefox 会话是相互关联的。在关闭 Virtual KVM Client 对话框之后，自动解除 Firefox 封锁。



索引

A

B

C

D

E

F

H

I

J

K

L

M

N

P



R

S

U

V

W

一划

二划

三划

四划

五划



六划



七划

八划

九划



十划

十一划

十二划

十三划

十四划



十六划



Raritan.

美国/加拿大/拉丁美洲

星期一至星期五
上午 8:00 - 傍晚 8:00　东部时间
电话：800-724-8090 或 732-764-8886
对于 CommandCenter NOC：按 6，然后按 1
对于 CommandCenter Secure Gateway：按 6，然后按 2
传真:732-764-8887
有关 CommandCenter NOC 的电子邮件：tech-ccnoc@raritan.com
有关其他所有产品的电子邮件：tech@raritan.com

中国

北京

星期一至星期五
上午 9:00 - 下午 6:00　当地时间
电话：+86-10-88091890

上海

星期一至星期五
上午 9:00 - 下午 6:00　当地时间
电话：+86-21-5425-2499

广州

星期一至星期五
上午 9:00 - 下午 6:00　当地时间
电话：+86-20-8755-5561

印度

星期一至星期五
上午 9:00 - 下午 6:00　当地时间
电话：+91-124-410-7881

日本

星期一至星期五
上午 9:30 - 下午 5:30　当地时间
电话：+81-3-3523-5991
电子邮件：support.japan@raritan.com

欧洲

欧洲

星期一至星期五
上午 8:30 - 下午 5:00　GMT+1 中欧时间
电话：+31-10-2844040
电子邮件：tech.europe@raritan.com

英国

星期一至星期五
上午 8:30 - 下午 5:00　GMT
电话：+44(0)20-7090-1390

法国

星期一至星期五
上午 8:30 - 下午 5:00　GMT+1 CET
电话：+33-1-47-56-20-39

德国

星期一至星期五
上午 8:30 - 下午 5:30　GMT+1 CET
电话：+49-20-17-47-98-0
电子邮件：rg-support@raritan.com

澳大利亚墨尔本

星期一至星期五
上午 9:00 - 下午 6:00　当地时间
电话：+61-3-9866-6887

台湾

星期一至星期五
上午 9:00 - 下午 6:00　GMT-5 标准时间 GMT-4 夏令时
电话：+886-2-8919-1333
电子邮件：support.apac@raritan.com